CYBER OODA:

TOWARDS A CONCEPTUAL CYBERSPACE FRAMEWORK

BY

MAJOR CHRISTIAN L. BASBALLE SORENSEN

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2010

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

LT COL JOHN H. DAVIS (Date)

_____

DR. JOHN B. SHELDON (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Christian L. Basballe Sorensen is student at the Air Force School of Advanced Air and Space Studies, Maxwell AFB, AL. Prior to this assignment he was commander of the 5th Communications Squadron, Minot AFB, ND. This squadron serves two strategic nuclear wings and maintains a communications infrastructure worth $41 million supporting a total force of 6000 base Active Duty, Guard and Civilians working at Minot AFB and the 8,500 square mile missile range.

Major Basballe received his commission and graduated with academic and military distinction from the United States Air Force Academy in 1997. He was given a scholarship from the Air Force Academy to attend Stanford University where he was granted a Master of Science degree in Engineering Economic Systems and Operations Research in 1998. He was granted a Master's of Business Administration with concentrations in Supply Chain Management and Information Technology from the Robert H. Smith School of Business, University of Maryland, in 2004. He has served as an air staff personnel analyst, JSTARS mission systems analyst, flight commander, expeditionary communications squadron commander, joint operations officer, MAJCOM action officer and branch chief and squadron commander.

ACKNOWLEDGEMENTS

I would like to thank Mr. John Garstka, author of many of the fundamental texts on Network Centric Operations, who helped further my thinking regarding the Candidate Cyberspace Engagement Model presented in Chapter 3. His willingness and patience to discuss my ideas, even when skiing to the top of mountains to find cell phone reception, is a testament to his tenacity and support of this research. I hope the progress in cyber thinking herein is up to his standards, that it could be is the highest praise I could receive.

I would also like to thank the faculty at the School of Advanced Air and Space studies for allowing me the freedom to roam the cyber landscape in search of thesis topics and eventually reigning me in towards a specific topic. In particular, Lt Col (Dr.) John Davis was instrumental in honing and refining the question into a manageable, but still long, academic piece. His numerous comments always made the finished product better. Dr. John Sheldon was source of inspiration, jokes, and all around good cheer during this year long journey. Our discussion were wide ranging and I always left his office with more questions than answers, which I've come to understand is much better than answers.

Additionally, I would be remiss if I did not mention the others who have helped along the way. Col (Dr.) Kometer and Dr. Dolman, for unknowingly reading some ideas presented in this thesis that were unceremoniously jammed into their respective course papers. Dr. Ray Buettner and colleagues at Naval Post Graduate school for critically reviewing the Candidate Cyberspace Engagement Model. Thanks to Col Shannon Kruse, Danette Wile, and Maj Bobby Meyers for taking the time to discuss their perspectives on the state of cyber operations and strategy. Additionally, a heartfelt thanks to all of the other students in SAASS class XIX who helped make this year intellectually and professionally rewarding.

Finally, and most importantly, to my wife who had to put up with me being home more than normal, but still being inaccessible much of the time. Her help, encouragement, cooking, and good cheer were the real highlights of my year. I look forward with anticipation to the day where I can spend more quality time with her and our new son.

ABSTRACT

Military operations have shown fantastic increases in speed, lethality, and effectiveness by employing cyberspace capabilities. The Network Centric Operations Conceptual Framework (NCO CF) has proven to be a useful analytic tool to explain why and how network effects can be such a powerful enabler in military operations. However, the man-made nature of cyberspace makes it different from the other warfighting domains, defines its boundaries, drives its utility and creates its vulnerabilities. This thesis seeks to determine if the NCO CF can be applied to cyberspace engagements despite these differences.

Acknowledging the primary differences between cyberspace engagements and traditional military operations, the Candidate Cyberspace Engagement Model provides a framework for understanding and tracking the specific actions, reactions, and causes of cyberspace exploitations and attacks. Although the primary conclusion of this thesis is that the NCO CF can be used to analyze cyberspace conflicts, insights from the Candidate Cyberspace Engagement Model lead to some important qualifications and updates that must be applied to the NCO CF before doing so.

The Candidate Cyberspace Engagement Model also demonstrates how crucial situational awareness, command and control, collaboration, and stealth are to cyberspace engagements. These insights suggest policy and operational changes to the way cyberspace is created, defended, and operated for the Department of Defense and other organizations.

CONTENTS

Illustrations

Tables

Figures

Introduction

We can thus only say that the aims a belligerent adopts, and the resources he employs, must be governed by the particular characteristics of his own position; but they will also conform to the spirit of the age and to its general character. Finally, they must always be governed by the general conclusions to be drawn from the nature of war itself.

Carl von Clausewitz

U.S. military power today is unsurpassed on the land and sea and in the air, space, and cyberspace. The individual Services have evolved capabilities and competencies to maximize their effectiveness in their respective domains. Even more important, the ability to integrate these diverse capabilities into a joint whole that is greater than the sum of the Service parts is an unassailable American strategic advantage.

Chairman of the Joint Chiefs of Staff,
Admiral Mike Mullen

Carl von Clausewitz conceptualized war as a continuation of politics by other means.[1] In its most violent form, war has always been a life and death competition to achieve a political aim. Admiral Mullen's quote above accurately describes the current military environment where the United States stands unsurpassed in traditional military power. However, competition between nation states endures with modern technology enabling one nation to pursue its goals by avoiding its

[1] Carl von Clausewitz, *On War*. Edited and translated by Michael Howard and Peter Paret. (Princeton, NJ: Princeton University Press, 1976), 88.

competitor's military strength. As General Mattis, Commander of United States Joint Forces Command states, "Any enemy worth his salt will adapt to target our perceived weakness."[2] Because of the complexities of today's global environment, enemies can use any of the aspects of national power (diplomacy, information, military, economics, and culture) to build their strength or target others' weaknesses. Daniel Bell put an economic twist on Clausewitz's famous quote when he said, "economics will have become the continuation of war by other means."[3] History shows that political and military power is built upon a foundation of economic power. As such, it is imperative that the United States understand, monitor, protect, and grow its economic power.

The revolutionary use of information is dramatically enhancing the United States' current economic and military power, adding over 38% of the growth in the US economy between 1995 and 2000.[4] The information revolution has impacted many aspects of life in networked countries including the United States. Overall, this revolution has been called the "Third Wave," "Information Age," and so on.[5] When applied to the economy it has been called the "Information Economy" or "Knowledge Economy." No matter what the current form of economy is called, the results clearly demonstrate that the United States economic base is now in large measure tied to intellectual capital and its application through information technology tools.[6]

---

[2] Joint Forces Command, *Joint Operating Environment,* 2008, *iv*.
[3] Daniel Bell, *The Cultural Contradictions of Capitalism*, (New York, NY: Basic Books, 1996), 330.
[4] Alessandra Colecchia, Paul Schreyer, "ICT Investment and Economic Growth in the 1990s: Is the United States a Unique Case?: A Comparative Study of Nine OECD Countries," Review of Economic Dynamics, Volume 5, Issue 2, April 2002, (http://www.tos.camcom.it/Portals/_UTC/Scenari/I001.pdf), 16.
[5] "Third Wave" was popularized by Alvin Toffler's book of the same title in 1980, while "Information Age" was codified by Emmanual Lallani and Margaret Uy's book *The Information Age* and the like emerged as part of the technorati lexicon in the 1990's.
[6] Department of Justice, Computer Crime and Intellectual Property Section, "Prosecuting Intellectual Property Crimes," 3rd ed, 2006, Chapter I, http://www.justice.gov/criminal/cybercrime/ipmanual/01ipma.html (accessed 7 May 2010). This Department of Justice manual sites the value of U.S. intellectual capital at

Likewise, the use of information and communications technology in the military has been equally astounding and is often referred to as a "Revolution in Military Affairs."[7] This revolution enhances the capabilities of US military forces to the extent that the number of fighters no longer matter as much as their capabilities do. A ten-to-one numerical advantage is not important when the outnumbered forces are a hundred times more capable. Like a giant cantilever, this information advantage provides the economic and military instruments tremendous leverage they would not otherwise have. On the other hand, leverage can be a dangerous thing as it can leave the user exposed to the risk of collapse if any weakness in the lever appears. Therefore, it is imperative that the United States understand, monitor, and protect its information advantage which undergirds its economic and military power.

There have been many efforts to understand exactly how and why information can dramatically enhance military power. Perhaps none of these efforts have been more successful than the Network Centric Operations Conceptual Framework (NCO CF). Covered in depth in the next chapter, the NCO CF draws many conceptual parallels to John Boyd's Observe, Orient, Decide, Act (OODA) loop to explain the decision making process.[8] The NCO CF provides a framework to "bridge the gap between the simplicity of the OODA loop and the complex reality of military decision making and execution" in a complex joint or coalition environment with many actors, organizations, echelons, and decision makers participating.[9] The NCO CF builds on the concepts in Boyd's model and improves its utility by adding specific attributes and metrics.

$5T, with additional patents, trade secrets, research, and proprietary information embedded throughout the rest of the economy worth much more. All of these items are potentially at risk through cyberspace vulnerabilities.

[7] As explained in Part I of John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age*, (Santa Monica, CA: Rand, 1997), 23-175.

[8] John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 35.

[9] John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0, 35.

These additions help analysts understand and explore the process of leveraging information through communications networks to enhance traditional military operations. Further, the NCO CF also shows how activities in the information, cognitive, and social domains interact to influence the physical domain where traditional military activities occur. Applied correctly, the NCO CF can also point to weaknesses and areas to improve the information advantage.

The information advantage has become so obvious and integral to military operations of the United States that adversaries have also started to build their own capabilities around information and communication technology. Paradoxically, the characteristics that make these technologies useful also allow adversaries to target and directly engage the information advantage of the United States. These information engagements have become so critical that the cyberspace medium in which they occur has been added as a new domain for US military operations. There are many similarities between traditional military engagements and cyberspace engagements. Just as military capabilities, such as a Marine Air Ground Task Force, are created, used, attacked, and defended, so can cyber capabilities be created, used, attacked, and defended. Likewise, insights may be garnered from analyzing cyberspace engagements using the NCO CF in the same manner that typical military capabilities have benefitted. In pursuit of that possibility, this thesis asks the question: can the Network Centric Operations Conceptual Framework be applied to engagements in cyberspace? Before seeking an answer, it is important to provide some background and define the key terms and attributes of cyberspace used in this study.

Background

The invention of the telegraph marked the first time that humans instantly transmitted data beyond their line of sight. Ever since this invention, society and the military have used the physical attributes of

the electromagnetic spectrum to consistently increase the reach, speed, and variety of communication. Radios, telephones, cell phones, and the Internet represent the modern platforms for communication using the electromagnetic spectrum. The United States Department of Defense Advanced Research Projects Agency (ARPA) created the first Internet connections, called ARPANET, to allow researchers in different locations using heterogeneous computers to send and receive software programs and research data using their computers.[10] In other words, ARPA created the Internet to provide utility and the same logic applies to modern cyberspaces as well. Today's Internet is an outgrowth of ARPANET and it is synonymous with cyberspace. The utility of cyberspace is created by building infrastructure, standardizing protocols, installing applications, and getting other people to use the same applications at other points on the network. Cyberspace's reach continues to grow and it increasingly enhances how the military conducts both business and military operations.

The primary benefits of cyberpower are realized in joint action which maximizes complementary, rather than merely additive, effects of military power.[11] Operation Iraqi Freedom (OIF) clearly demonstrated how cyberpower can be used to play a leading role for military operations and other forms of power. For example, during OIF the United States attacked the cellular and computer networks used by insurgents to plan and plant roadside bombings. The cyber warriors executing this attack commandeered the insurgents' communications systems and planted false instructions which ultimately led insurgents into "the fire of waiting US soldiers."[12] Some officials have gone so far as to state that these

---

[10] "ARPANET – The First Internet," http://www.livinginternet.com/i/ii_arpanet.htm (accessed 27 May 2010). ARPA is the predecessor to DARPA as it is known today.
[11] Department of Defense, "Capstone Concepts for Joint Operations," v3.0, 15 Jan 2009, http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf, 24.
[12] Shane Harris, "The Cyberwar Plan," *National Journal Magazine*, 14 Nov 2009, http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed 14 Dec 09).

types of cyber-attacks allowed the military to capture and kill some of the most influential insurgents and may have turned the tide of the conflict as much as or more than the 2007 surge.[13] Understanding the foundations of cyberspace will help joint military planners envision future combined arms actions integrating cyberspace capabilities.

Cyberspace foundations: physical, syntactic, and semantic layers

Before cyberspace can provide utility at a specific place, three distinct layers must be created and working together: the physical layer, the syntactic layer, and the semantic layer.[14] These words are rooted in linguistics and have similar meaning in cyberspace. Each layer possesses distinct attributes that when integrated and operating correctly, allow for meaningful interaction through cyberspace.

The first requirement to build a cyberspace is the physical layer, which comprises all of the hardware required to send, receive, store, and interact with and through cyberspace. This infrastructure includes items such as cables, routers, transmitters, receivers, disk drives, computers, and interface devices. It is the bridge between the medium used to transit cyberspace, in the form of airwaves and fiber optic or copper cables, and the syntactic layer. The creation of a physical connection creates the potential for syntactic exchange.

The syntactic layer uses protocols and software that have been created to send, receive, store, format, and present data through the physical layer. This layer can be further broken down into sub-layers, such as the seven layers of the Open System Interconnection (OSI) Reference Model. [15] While these sub-layers can be individually targeted

---

[13] Harris, "The Cyberwar Plan."
[14] Derived from Martin Libicki's, *Conquest in Cyberspace: National Security and Information Warfare*, (Cambridge MA: Cambridge University Press, 2007), 8-9.
[15]Cisco Systems Inc., "Internetworking Basics," http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html (accessed 27 May 2010). However, it is important to note that different sub-layers of the syntactic layer may have different types of vulnerabilities depending on the characteristics of the sub-layer protocol that is used.

during a cyber-engagement, doing so is a matter of tactics and they are not considered further in this paper. Both the physical and syntactic layers must be working in order to have a potentially useful information exchange with any network node or termination point.

The semantic layer is all about the information presented to humans or machines. For information to be meaningful, it may have format, language, timeliness, or accuracy requirements. Additionally, for most military communications, this information should also be secure. Secure information should follow the principles of information security including confidentiality, integrity, availability, authenticity, and non-repudiation.[16] The trade-off between speed, cost, complexity, and security is an important consideration when constructing and using information systems.

If all three layers are working, the information delivered has the potential to provide utility. The relationship between the potential utility and the physical, syntactic, and semantic layers at one node of a cyberspace is represented by Figure 1 below:

[16] The Office of the Assistant Secretary of Defense for Networks and Information Integration, "DoD Information Assurance Strategic Plan," August 2009, 1, http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf (accessed 27 May 2010).

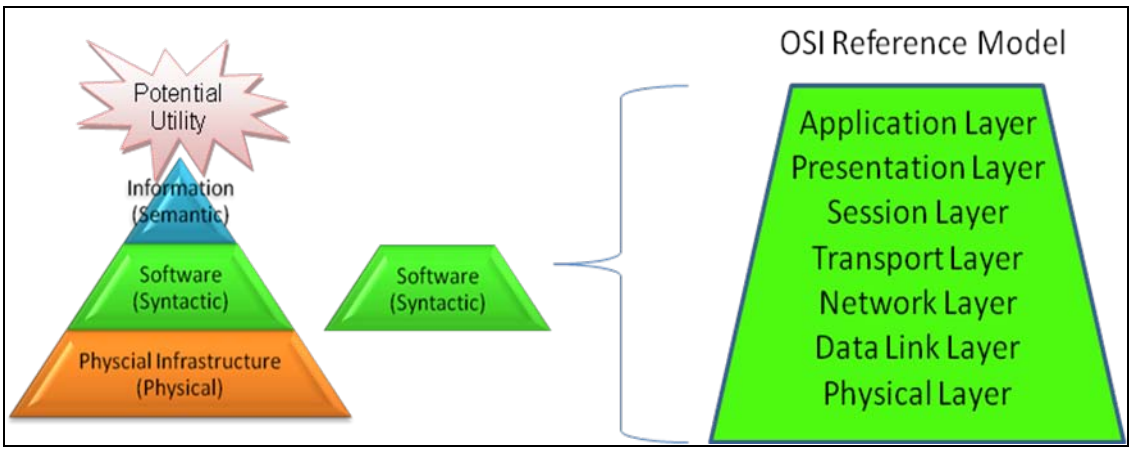


Figure 1: Graphical Illustration of Components Required to Deliver Potential Cyberspace Capability at a Single Node
(Adapted from Daniel T. Kuhn in "From Cyberspace to Cyberpower: Defining the Problem" in *Cyberpower and National Security* ed. Franklin D. Kramer et al. (Dulles, VA: National Defense University Press and Potomac Books, 2009), 33, Martin Libicki's Physical, Syntactic and Semantic layers defined in *Conquest in Cyberspace: National Security and Information Warfare* (New York, NY: Cambridge University Press, 2007), 8-9, and the OSI Reference Model information was assembled from Cisco Systems Inc., "Internetworking Basics," http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html (accessed 27 May 2010). The potential utility figure at the top-left of the graphic was added by the author.)

If any of the layers is missing, unintelligible, or malfunctioning at a particular point on the network, a meaningful interaction will not occur at that point, thus diminishing or completely removing the network's potential utility. All three layers working together at a node is described as the "entry fee" in the NCO CF.[17] An important corollary is observed in dense networks with many paths; meaningful exchanges may be routed around a non-working routing node, but the network cannot deliver to a non-working node. Further, one working node does not make a network. There must be at least one transmitting and one receiving node in order to create a valid cyberspace and to enable information exchange.

[17] John GarstkaEvidence Based Research, "Network Centric Operations Conceptual Framework," ver 1.0, November 2003, 2.

Once two or more nodes are working together, each node complements every other node to make the sum of the whole greater than the parts. In economic terms, the addition of another node represents positive network externalities, otherwise known as network effects, where a bigger network is to everyone's benefit.[18] The utility of the network increases in a non-linear fashion as the number of functioning nodes increases. Generally more open systems stand to benefit from network effects, although there might be some very good reasons for limiting the openness of a network.

The "potential" qualifier for each level also sets an upper limit that cannot be exceeded for each layer. For example, the potential limit of the physical layer is easy to understand in terms of bandwidth or the range of a cell tower. The limits of the physical layer constrain the utility of the syntactic and semantic layers in that cyberspace. Likewise, the syntactic layer can be constrained by the type of application, out of date software, or incompatible protocols. Examples include attempting to launch I-tunes on a Windows 95 computer (incompatible), attempting to go to a website that has been blocked by firewall settings (cannot view), or a combination of physical and syntactic limits, or viewing a content-rich PowerPoint presentation on a blackberry (viewable at low resolution, slow speeds, and cannot edit). Similar logic applies to the semantic layer where the potential utility may be constrained by the format of the data (e.g. receiving an image instead of an editable object with meta-data) or the organization of the data (e.g. a website layout where users can't find useful information because it's poorly structured). Additionally, the potential utility of the node and the information received is not only constrained by all of the limits of the layers described above, but also by the cognitive and social ability of the user receiving it.

---

[18] Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Boston, MA: Harvard Business School Press, 1999), 183.

The cognitive domain translates information into knowledge, intelligence, and decisions. The social domain is where individuals share information and collaborate to build understanding, discuss actions, and make collective decisions. Returning to John Boyd's OODA loop, commanders can still make poor decisions even if the information is presented superbly during the observe step and they properly orient themselves. This let-down is due to numerous cognitive, social, temporal, environmental, and organizational factors surrounding the decision maker. The complications explained above show that cyberspace is not a silver bullet that can solve problems regardless of the context of the cognitive, social, and physical domains. With these foundational elements defined, a working definition of cyberspace can be constructed.

Definition of Cyberspace

While it is conceptually easy to see and feel how the land, sea, and air domains are separate and distinct from one another. It is quite another matter to explain how an information exchange between machines is also a separate and distinct domain where "the concepts of length, width and height of land, sea, air and outer space, have all lost their significance."[19] As a result, there are numerous and diverse definitions of cyberspace among authors and organizations. For the purposes of this paper, cyberspace is defined as an environment created when computers utilize the physics of the electromagnetic spectrum to exchange and use information.[20] An important implication of this definition is the fact that there can be separate instances of cyberspace concurrently in the same geographic point. For example, an office with a

---

[19] Liang, Qiao and Wang Xiansui, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, 1999), 42, http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf.

[20] This definition draws from aspects of Gregory Rattray, Walter Sharp and the 2006 National Military Strategy's definitions in David Kuehl "From Cyberspace to Cyberpower: Defining the Problem" in *Cyberpower and National Security* (Washington DC: Potomac Books, 2009), 26-29.

LAN connection, a virtual private network (VPN) connection to a remote private network, cell phone connectivity, and digital two-way radio, represent four distinct cyberspaces if they cannot interact with each other.[21] These cyberspaces must be considered separate until a physical or syntactic mechanism is created, available, and used to connect separate cyberspaces. The connecting mechanism is vital to understanding not only how cyberspaces are created, controlled and used, but ultimately their power and vulnerability. A graphical representation of a cyberspace is shown in Figure 2 below:

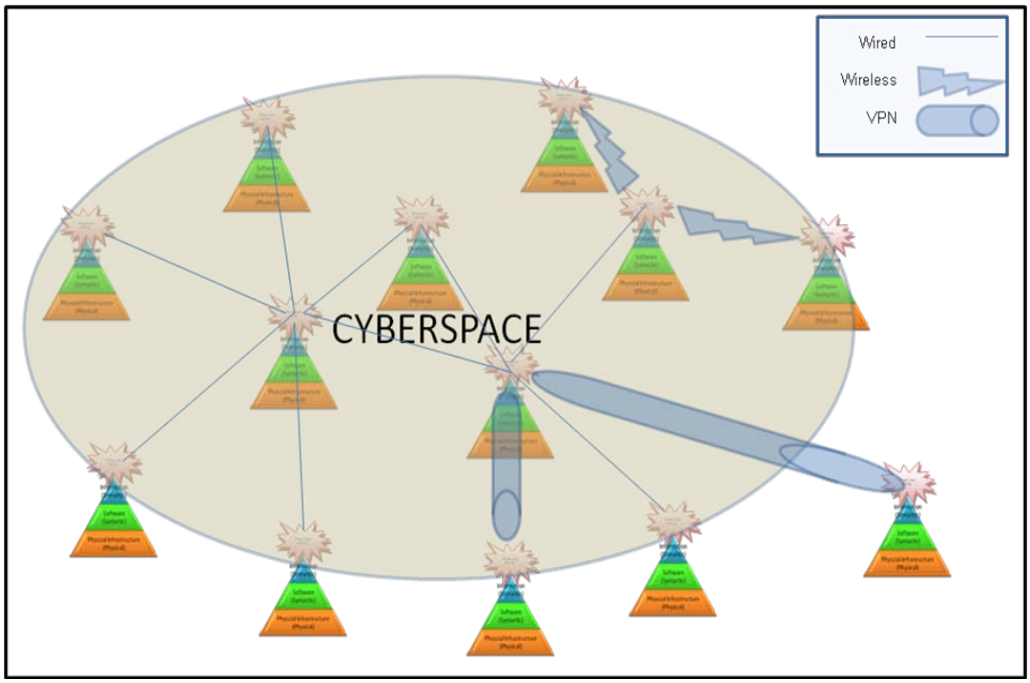


Figure 2: Graphical Illustration of a Cyberspace Composed of Compatible Nodes
(Source: author's original work)

[21] This is an ideal type definition. VPNs tunnel through traditional networks, but do not exchange information other than travel instructions. As long as the VPN tunnel remains secure, it is treated as a separate cyberspace. If security breaks down logical cyberspaces will merge into a single cyberspace.

Definition of Cyberpower: Leveraging Network Effects Through Cyberspace

The electric energy used to transmit information is the motive power and the use of information is the purpose of cyberspace. Although data is not an activity per se, it is the enabler and informer of all activities in cyberspace. In their seminal book, *Information Rules*, Shapiro and Varian explain that the power of information is derived from network effects.[22] Distinct from the normal economic thought of linear economies of scale, network effects increase the total value of the network in a non-linear fashion as the number of network nodes grows. Additionally, since information can be copied and distributed with virtually zero cost, cyberspace can provide tremendous utility wherever it can be accessed.

In the other warfighting domains, power is derived from human's ability to use tools to manipulate the domain to their advantage. The same logic applies to power in cyberspace. A useful definition of cyberpower is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[23] Traditionally, military cyberpower is used to increase shared situational awareness, increase the effectiveness of command and control, and make weapons more accurate.[24] Even cyber skeptics like David Lonsdale concede that "a digitized force should be better able to co-ordinate its operations and thereby operate at a higher tempo" if it so desires.[25] Alternatively, a commander using cyber attack and exploit tools against a digitized enemy may be able to reduce the

---

[22] Shapiro and Varian, *Information Rules*, 183.
[23] Kuehl, "From Cyberspace," 38.
[24] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington, DC: DOD, 2005), 21.
[25] David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 92.

enemy's access to information, raise the enemy's uncertainty, and obtain better intelligence regarding enemy capabilities and intentions.[26]

Overview of thesis

This study has three primary areas. First, chapter 1 provides an overview of the NCO CF. The NCO CF is a conceptual representation of the network value chain as it crosses the information, cognitive, social, and physical domains. It expands Boyd's OODA loop and presents a detailed model describing the process of transforming raw data into information, information into situational awareness, and situational awareness into better decisions which ultimately lead to increased mission effectiveness. Additionally, it provides tools for measuring and evaluating the performance of each of the steps along the way. While, the NCO CF has previously been used to compare the effectiveness of network enabled units against traditional military units during kinetic military operations, chapter 2 turns to focus on the cyberspace domain. This chapter explains some of the limits of the NCO CF as it applies to cyberspace. This analysis will also explore the differences between traditional military engagements and cyberspace engagements to see how the NCO CF needs to be modified to analyze engagements occurring in cyberspace. Chapter 3 tackles these limitations directly by presenting a Candidate Cyberspace Engagement Model which provides a framework for understanding how and why activities in cyberspace occur. The candidate model is itself an exploration of the NCO CF concept of "networked forces." The candidate model provides the reader with a richer understanding of the cyberspace environment and a framework for evaluating the interactions and challenges of operating in this unique environment. Finally, chapter 4 goes to the heart of the thesis by leading the reader through some important qualifications and NCO CF updates required before this framework can be applied to cyberspace

[26] Director, Force Transformation, Implementation of Network-Centric Warfare, 8.

engagements. The conclusion summarizes the arguments of the thesis and also suggests follow-on research to further understand this burgeoning area of warfare.

Chapter 1

Network Centric Operations Conceptual Framework

> *To succeed, it will not be sufficient to simply intensify existing management strategies. Leaders must think differently about how to compete and be profitable, and embrace a new art and science of collaboration … we are talking about deep changes in the structure and modis operandi of the corporation and our economy, based on new competitive principles such as openness, peering, sharing, and acting globally.*
>
> Don Tapscott and Anthony Williams in *Wikinomics*

> *In armed conflict no success is possible – or even conceivable – which is not grounded in an ability to tolerate uncertainty, cope with it, and make use of it.*
>
> Martin van Creveld in *Technology and War*

Information and communication technologies have changed the world as we know it. However, humans have not yet achieved a widespread conceptualization of information's potential power. If we are in the midst of an information revolution, the complexity and dynamism of the current environment may represent the blood and chaos in revolutions of old. The military has expressed the potential of this revolution through concepts like Information Superiority and Decision Dominance, but it has yet to fully understand the logic and information mechanics that create this potential. The Network Centric Operations Conceptual Framework (NCO CF) attempts to build and test the current concepts of creating, delivering, and using information to deliver battlefield effects.

The NCO CF evolved from thinking regarding the use of information in warfare. This evolution was accelerated in the 1990s through the work of the Command and Control Research Program (CCRP), the publication of Joint Visions 2010 and 2020, and the stand-up of the Office of Force Transformation. VADM Cebrowski and John Garstka in their seminal article titled "Network Centric Warfare: Its Origin and Future," describe Network Centric Warfare (NCW) as an outgrowth of "the co-evolution of economics, information technology, and business processes" reflected in society to produce value through "the content, quality, and timeliness of information moving between nodes on the network."[1] This writing presented a new concept for military operations that "derives its power from the strong networking of a well-informed but geographically dispersed force."[2] A year later, under the auspices of the CCRP, the book *Network Centric Warfare: Developing and Leveraging Information Superiority* assembled much of the thinking regarding information warfare and network-centric warfare up to that point. It delved deeper into the power of information age organizations and translated the logic of that power to the potential of a network-centric military. It also compared the commercial and potential military network value chain as illustrated in figure 3 below.[3] Network Centric Warfare's potential is not fully understood nor completely adopted in formal military publications, although the CCRP research has made significant progress towards understanding it.

---

[1] VADM Arthur K. Cebrowski, USN, and John J. Garstka, "Network Centric Warfare: Its Origin and Future," *Proceedings of the Naval Institute* 124, no. 1 (January 1998), accessed through http://www.kinection.com/ncoic/ncw_origin_future.pdf, p. 1-2, (accessed 8 March 2010).
[2] Cebrowski and Garstka, "Network Centric Warfare," 9.
[3] David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare*, 2nd ed (Washington, DC: CCRP, 1999), 36 and 89.

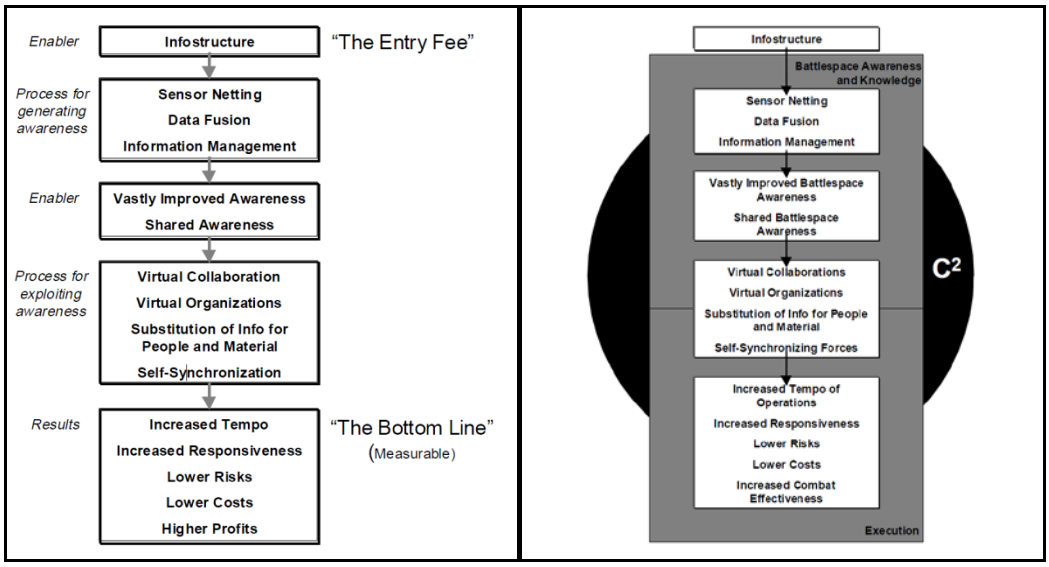


Figure 3 – The Network Centric Enterprise and Network Centric Military
(Reprinted from David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare*, 2nd ed (Washington, DC: CCRP, 1999), 36 and 89).

Joint Vision 2020, published in 2000, extended the discussion of the information superiority concepts initially highlighted four years earlier in Joint Vision 2010. Importantly, Joint Vision 2020 recognized the conceptual link between NCW and information superiority by stating "the global information grid will provide the Network Centric environment required to achieve" the goal of a "fully synchronized information campaign."[4] The global information grid is the "entry fee" proposed in *Network Centric Warfare* as a necessary prerequisite to conduct NCW. With these foundational documents and additional research continuing to accrue, John Garstka led a team from Evidence Based Research Inc. in 2003 to expand and contextualize the original NCW tenets. The NCO CF resulted from this initiative. The NCO CF was developed to build "a rich and comprehensive set of NCW related metrics that could be used in

[4] Cebrowski and Garstka, "Network Centric Warfare," 9.

experimentation and other research endeavors to gather evidence." [5] This evidence could be used to inform investment decisions across DoD doctrine, organization, training, material, leadership, personnel and facilities (DOTMLPF). . The NCO CF has subsequently been used to make sense of the logic of Network Centric Operations.

NCW Tenets: Origin of Network Centric Operations Conceptual Framework

A 2001 report to Congress formally expressed the tenets of NCW. These tenets build on the ideas presented in *Network Centric Warfare* and were stated as follows: [6]

-- A robustly networked force improves information sharing.

-- Information sharing enhances the quality of information and shared situational awareness.

-- Shared situational awareness enables self-synchronizations, and enhances sustainability and speed of command.

-- These, in turn, dramatically increase mission effectiveness.

The NCW tenets present a string of interrelated hypotheses for explaining the process and logic behind how network capability improvements eventually lead to mission effectiveness. The NCW tenets, as articulated above, make logical sense, but neither present concrete causality nor explain how to best implement NCW. Analysts and planners must model the tenets and their linkages with analytical rigor in order to increase their understanding of why these tenets are true and explain how to best take advantage of them in the future.

Value Chain: Basic Model of NCW Tenets

Bringing the NCW tenets together into an integrated concept, analysts can begin to understand how and where information is collected and subsequently used to make decisions to achieve battlefield effects.

---

[5] John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 2.

[6] Department of Defense, *Network Centric Warfare Report to Congress*, July 2001, 57, http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf (accessed 8 Mar 10).

The Network Centric Value Chain is a visual model of the NCW tenets and an important step towards understanding the power of information. The initial Network Enabled Value Chain in figure 4 below maps the NCW tenets across the four domains.

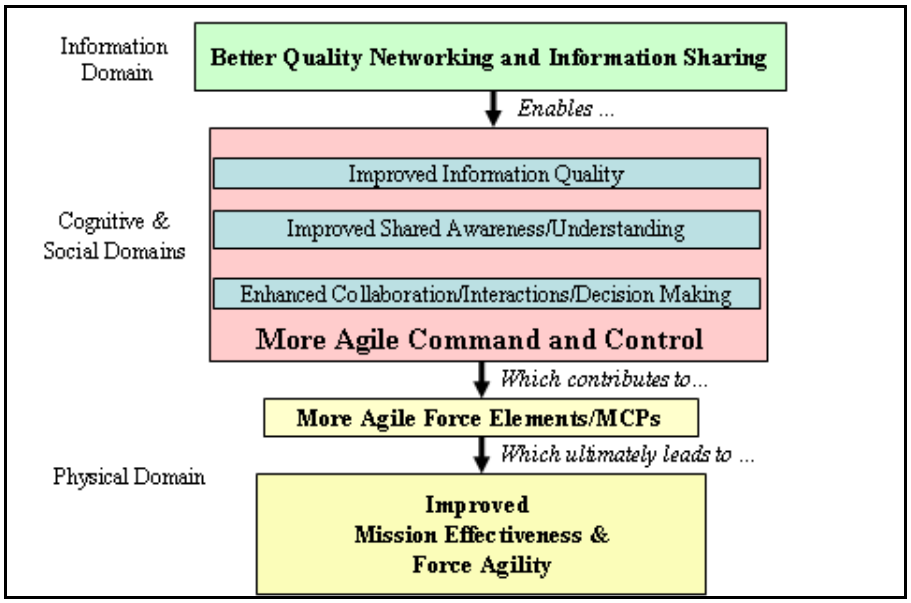


Figure 4 – Network Enabled Value Chain
(Reprinted from: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 10).

From Warfare to Operations

Network Centric Operations (NCO) replaced the NCW vernacular in 2003 to "counter the view that Network Centric concepts and capabilities were only applicable to high-end combat; rather that it was applicable to the full mission spectrum including non-kinetic missions."[7] Network Centric Operations is a collection of powerful organizational and technical concepts. On the organizational side, it posits that organizations are more effective when they bring "power to the edge," that is, when they make information freely available to those who need it and permit free collaboration among those who are affected by or can

[7] David Alberts, "NEC2 Short Course – Module 2 Network-Enabled Capability," page 12, *http://www.dodccrp.org/files/nec2_short_course/NEC2%20Short%20Course%20Module%202%20-%20NEC2%20-%20%20Alberts%201-%2024%20-2010.pdf*, (accessed 8 Mar 2010).

contribute to a mission.[8] This freedom brings the operational benefits of better and more widespread understanding of the commander's intent, better self-synchronization of forces in planning and operations, fuller freedom of movement with better information, and the ability to harness worldwide resources on a global information grid without the need to bring all of those resources forward into the area of operations.[9] The NCO CF expands on the original NCW tenets and adds analytical rigor for evaluating the Network Enabled Value Chain. Later, this chapter explains each of the major components of the NCO CF in turn.

Comparing the NCO CF to the OODA Loop

John Boyd's Observe, Orient, Decide, Act (OODA) loop represents a popular military conceptualization of the modern warfighting process. Boyd's cyclical process focuses on the mind of the commander as he or she continuously gathers information in the observe step, relates the new information to their worldview in the orient step, decides what to do, and gives orders for the force to act. Boyd's loop accomplishes two innovations. First, it articulates the feedback process of decisions, actions, and observations back into observe step throughout a cyclical decision making process. Second, it starts to zero in on the complexity involved in orienting one's mind to take appropriate action. This orientation can be influenced by a number of factors: previous experiences, genetic heritage, cultural traditions, new information, and the personal or organizational dialectic process used to analyze and synthesize inputs to make decisions in a dynamic environment.[10] Figure 4 shows Boyd's OODA loop.

---

[8] This phrase was popularized by David Albert and Richard Hayes book *Power to the Edge: Command and Control in the Information Age*, (Washington, DC: CCRP), 2003.
[9] Jeremy Kaplan, "A New Conceptual Framework for Net-Centric, Enterprise-Wide, Systems-of-Systems Engineering," (Washington: DC, Center for Technology and National Security Policy, National Defense University, June 2006), 5.
[10] David Fadok, "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory,* ed. Col Phillip Melinger (Maxwell AFB, AL: Air University Press, 1997), 366-367.

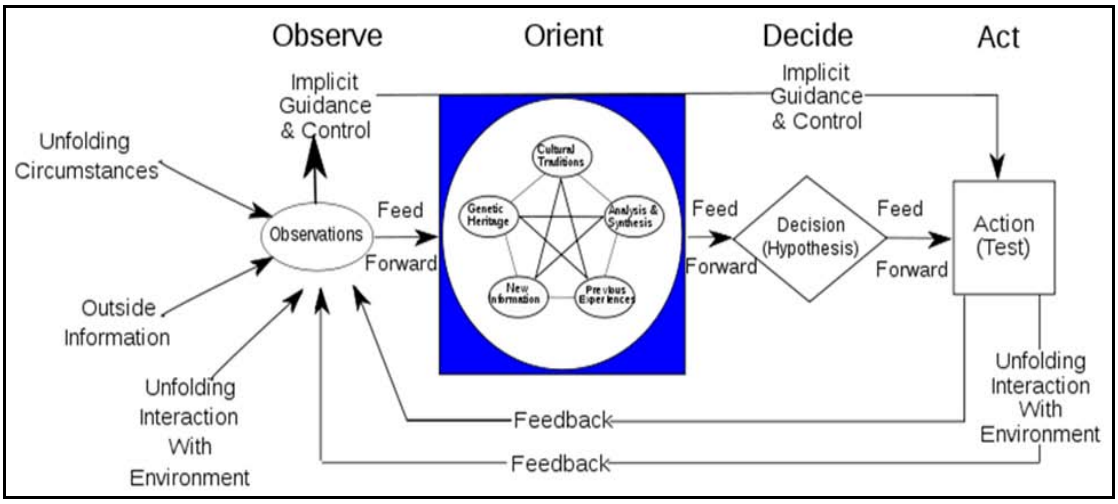


Figure 5 – John Boyd's OODA Loop
(Reprinted from Grant Hammond, *The Mind of War: John Boyd and American Security*, 190)

The NCO CF expands on Boyd's concepts by showing how and why Boyd's steps can work or be inhibited by the process involved. Boyd's Observe step is represented by the NCO CF concepts of information sources, command and control, organic information, quality of networking, degree of information share-ability, and quality of individual information. The NCO CF breaks the complexity of the Boyd's Orient step into the concepts of individual and shared awareness, quality of interactions, and individual and shared understanding. The NCO CF also breaks Boyd's Decide step into quality of interactions, individual and collaboration decisions, as well as decision synchronization across the force. Finally, the NCO CF expands Boyd's Act step into command and control agility, degree of entity synchronization, and degree of effectiveness which feed back into Boyd's Observe step. By taking Boyd's loop apart in an analytical and rigorous way, the NCO CF can provide great insights into the reasons why operations occur in the manner they do, as well as predict the effectiveness of targeted upgrades.

Presentation of the Conceptual Framework

The NCO CF is an expanded view of the original NCW tenets and the network value chain presented above. It models in detail the process

of transforming raw data into information, information into situational awareness, and situational awareness into better decisions, ultimately leading to increased mission effectiveness. The NCO CF consists of three major components: the military force conducting operations; the operating environment represented by physical, information, cognitive, and social domains; and the expanded network value chain consisting of eleven interacting concepts comprising network-centric operations theory. Each of these three components are explored further below, with the explanations of the eleven network-centric concepts dominate this exploration. Figure 6 illustrates the major components and flow of the NCO CF and is a good reference for the remaining NCO CF discussion.

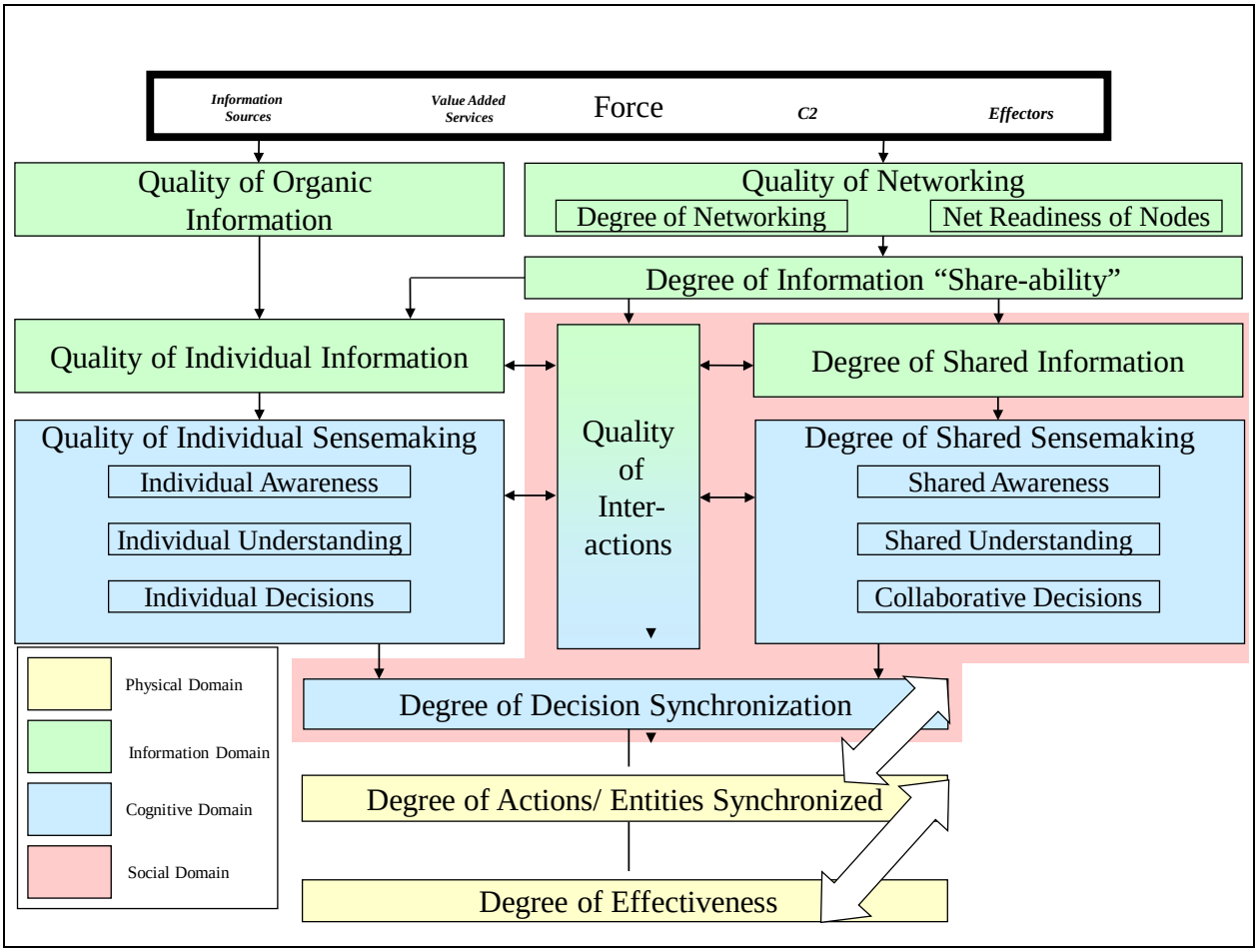


Figure 6 – Overview of Network Centric Conceptual Framework
(Reprinted from: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 10)

The Force

The force portion of the NCO CF, shown at the top of figure 6, represents the military resources available for action and it includes the resources and processes deployed to accomplish the mission. Inside the NCO CF the force performs four functions: sensors collect the raw data, value added services process the data into information or intelligence and distribute it across the network, command and control elements, and effectors—"the war fighters, weapons and other systems that can physically destroy the enemy or affect other elements" in the operational environment.[11]

The force should be considered the input that is used by military decision making and action to create battlefield effects. It is also important to note that a single platform can provide more than one function. For example, an F-22 can gather raw intelligence, conduct command and control activities, and destroy targets during the course of a single mission. At the end of the NCO CF, forces receive the output of shared decisions to implement military action.

The Four Domains

As seen in figure 6, the NCO CF operates in and through the physical, information, cognitive, and social domains. Military forces strike, protect, and maneuver in land, sea, air, and space environments within the framework's physical domain. Information is created, manipulated, value-added, and shared in the framework's information domain. Forces build awareness, perceive, understand, decide, and hold beliefs and values within the cognitive domain. These intangible concepts are crucial elements of network-centric operations. The NCO CF is differentiated from Boyd's OODA loop because it includes the social domain where forces interact, exchange information, awareness, and understanding, and make collaborative decisions. This domain overlaps

[11] Daniel Gonzales et al., *Network Centric Operations Case Study: Air-to-Air Combat With and Without Link 16*, (Santa Monica, CA: RAND, 2005), 3.

with the information and cognitive domains, but is distinct from both. Cognitive activities are inherently individualistic and occur in the minds of individuals. On the other hand, shared sensemaking (the process of going from shared awareness, to shared understanding, and to collaborative decision making) can be considered a socio-cognitive activity since the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa.[12] Figure 3 represents these domains in different colors, as depicted in its legend.

Top Level Concepts and Their Attributes

The NCO CF not only adds fidelity to top-level concepts of the network value chain, but it also describes each top level concept shown in figure 6. Further details, not shown in figure 6 but explained in the NCO CF, quantify each top level concept through a set of measurable attributes. These attributes represent theoretical extensions of the network-centric hypothesis and have been useful for evaluating the outcomes of network-centric forces. The attributes can assess their respective concepts using objective and subjective metrics to measure quantity (how much, frequency, how long, etc.) and quality (how correct, how appropriate, how complete, etc.).[13] Objective attributes can measure the quality of processes in reference to criteria that are independent of the situation and apply across the breadth and scope of the situations the force may face. Since they are independent of the situation, the objective attributes can also be repeated—an important criterion for experimentation and testing purposes. The contextual attributes, called "fitness for use attributes" in the NCO CF, measure quality with respect to "the demands of the specific situation."[14] For example, accuracy needs to be within a few meters for targeting

---

[12] John Garstka, "Network Centric Operations Conceptual Framework," ver 1.0, November 2003,10.
[13] John Garstka, "NCO CF," ver 1.0, 6.
[14] John Garstka, "NCO CF" ver 2.0 (draft), June 2004, 115.

purposes, but only a couple of kilometers within the context of tracking the general direction of large enemy movements.

The concepts are closely linked and flow in a logical, but interactive manner to contribute to the dependent variable of mission effectiveness.[15] The NCO CF typically compares the effectiveness of traditional military units against network-enabled units during kinetic military operations. This comparison helps to identify and describe how and why network-enabled forces are more effective. Each top level concept is explained below starting with the quality of organic information concept shown at the top of Figure 6.

Quality of Organic Information Joint Publication 1-02 defines organic as being "assigned to and forming an essential part of a military organization."[16] Applying this definition to information, the concept of organic information can be understood to be "information derived from or gathered by a (military force) entity that is not shared and is unavailable to the network" at the point of origin.[17] This concept is an assessment of the capability of force entities to generate raw data at the edges of the network. Importantly, the concept is concerned only with the local capability to generate quality data and not with the availability of data elsewhere, as this is addressed directly in the "degree of information shareability" concept. The concept is assessed through the following four objective attributes and four contextual attributes.

---

[15] John Garstka, "NCO CF," ver 1.0, 14.
[16] DoD Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/dod_dictionary/ (accessed 6 Mar 2010).
[17] John Garstka, "NCO CF," ver 2.0 (draft), 109.

Table 1 – Quality of Organic Information Attributes

Objective Attributes	
Correctness	Extent to which information is consistent with ground truth.
Consistency	Extent to which information is consistent with prior information.
Currency	Age of the information.
Precision	The level of fidelity in the data.
Contextual Attributes	
Completeness	Extent to which relevant information that has been collected.
Accuracy	Degree to which the precision matches what is needed.
Relevance	Proportion of information collected that is related to the task at hand.
Timeliness	Degree to which currency matches what is needed.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 109-110.

These attributes attempt to evaluate how much the information can help decision making.

Quality of Networking This concept "refers to the extent of interconnection among force entities."[18] Networking is a critical enabler for the information domain. It is conceptually composed of both the infrastructure facilitating the interaction, which is the network, and the nodes that are capable of interacting with other nodes across the infrastructure. Measuring the overall quality of the network requires assessing both the network infrastructure and the net readiness of the nodes as seen in tables 2 and 3 respectively.

[18] John Garstka, "NCO CF," ver 1.0, 28.

Table 2 – Degree of Networking Attributes

Attributes	
Reach	Percent of nodes can communicate in desired access modes, formats, and applications.
Quality of Service	Ability of the network to provide a variety of communication services.
Network Assurance	Extent to which network provides services that facilitate the assurance of information in the areas of privacy, availability, integrity, authenticity, and nonrepudiation.
Network Capacity	Measure of how large the network can get before degradation in quality of service and throughput occurs.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 105-106.

Table 3 – Net Readiness of the Nodes Attributes

Attributes	
Node Assurance	Extent to which node supports facilitate information assurance services.
Capacity	Maximum ability of node to exchange data = throughput.
Agility: Robustness	Ability of node to connect with network across a range of operational conditions (environments and mission types).
Agility: Flexibility	Number and type of connectivity modes supported.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 108.

The NCO CF contains attributes and metrics for each, but does not directly assign contextual attributes at this stage in the NCO CF's development.

Degree of Information "Shareability" This concept describes the ability of individual forces to share organic information with other forces quickly and accurately. Shareability bridges the conceptual gap between organic and non-organic information inside the network. It assesses the degree to which fielded forces can post their organic information to the network and the extent to which that information can be discovered by other forces. This concept considers how well the posted information is

indexed, if it is stored as it is intended, transmitted accurately and when needed, and presented to the receiver in a manner equivalent to what was submitted.

Table 4 – Degree of Information Shareability Attributes

Objective Attributes	
Quantity of Posted Information	Percent of collected information that is posted to the network.
Ease of use of Posted Information	Amount of information which is in a format that facilitates use across a range of possible applications. Dependent upon the extent of indexed meta-data and application independent data on the network.
Retrievably of Information	Extent to which the posted information is easily retrieved. Determined by the following three characteristics: entity awareness of the information, access to the information through search or rights, and meta-data describing what the information is and how it may be used.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 108.

Quality of Individual Information The authors of the foundational book, *Understanding Information Age Warfare*, concluded that force "entities will be conceived and built net-ready to connect, with the presumption that they will increasingly depend upon non-organic information for their preferred mode of operation."[19] Conceptually dependent on the quality of organic information, degree of information shareability, and the quality of interactions, Quality of Individual Information can viewed as an aggregation of the data posted and available from all organic data sources in the network. Specifically, this concept represents the quality of the information that an individual possesses "from all sources, whether generated organically, transmitted

[19] David Alberts et al, *Understanding Information Age Warfare*, (Washington, DC: Command and Control Research Program, 2001), 29.

over the technical network, or heard in a conversation."[20] The Quality of Individual Information concept shares all the same attributes as organic information, but includes non-organic information in the assessment of those attributes and also adds the uncertainty attribute. Uncertainty is likely to build when multiple information sources are inconsistent. As shown in Figure 6, this concept provides the informational basis for individual sensemaking.

Table 5 – Degree of Information Shareability Attributes

Objective Attributes	
Correctness	Extent which information is consistent with ground truth.
Consistency	Extent which information is consistent with prior information.
Currency	Age of the information.
Precision	The level of fidelity in the data.
Contextual Attributes	
Completeness	Extent to which relevant information that has been collected.
Accuracy	Degree to which the precision matches what is needed.
Relevance	Proportion of information collected that is related to the task at hand.
Timeliness	Degree to which currency matches what is needed.
Uncertainty	Individual's perception of information uncertainty.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 111.

Degree of Shared Information The first concept occurring in the social domain, this concept assesses the information that is generated and available to fielded forces. Whereas the degree of information

[20] Daniel Gonzales et al., Link 16 Case Study, 5.

shareability concept assesses the potential to share information, this concept assesses the implementation and use of this potential. The attributes for this concept match those of organic information, but also include the attribute of extent to measure how widely across the force organic information is shared.

Table 6 – Degree of Shared Information Attributes

Objective Attributes	
Extent	Proportion of information in common across force entities. Proportion of force entities that share an information item.
Correctness	Extent to which information is consistent with ground truth.
Consistency	Extent to which information is consistent with other relevant information and prior information from the same source.
Currency	Age of the information.
Precision	The level of fidelity in the data.
Contextual Attributes	
Completeness	Extent to which relevant information that has been collected.
Accuracy	Degree to which the precision matches what is needed.
Relevance	Proportion of information collected that is related to the task at hand.
Timeliness	Degree to which currency matches what is needed.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 111.

Quality of Individual Sensemaking Conceptually and intricately linked to quality of individual information and quality of interactions, this concept begins to explore the NCO CF activities occurring in the cognitive domain. It assesses an individual's ability to take the information presented and make a useful decision. This key concept relies on three sub-components. The first, individual awareness,

describes how well an individual can interpret the information received in terms of mission, constraints, environment, and capabilities and intentions of opposing and neutral forces. Individual awareness is measured through the following objective and contextual attributes:

Table 7 – Degree of Individual Awareness Attributes

Objective Attributes	
Correctness	Extent which awareness is consistent with ground truth.
Consistency	Extent which awareness is consistent with relevant awareness at an earlier time period.
Currency	Time lag of awareness.
Precision	The level of granularity of awareness.
Contextual Attributes	
Completeness	Extent to which awareness necessary to form understanding is obtained.
Accuracy	Appropriateness of precision of awareness for a particular use.
Relevance	Extent to which awareness is related to task at hand.
Timeliness	Extent to which currency of awareness is suitable to use.
Uncertainty	Subjective assessment of awareness uncertainty.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 116.

The quality of individual understanding, the second sub-component of individual sensemaking, assesses the ability of an individual "to infer meaning from their mental view of the battlespace to include recognition of patterns, dynamic futures, and opportunities and risks."[21] The quality of individual understanding is measured through the following attributes:

[21] Daniel Gonzales et al., Link 16 Case Study, 5.

Table 8 – Quality of Individual Understanding Attributes

Objective Attributes	
Correctness	Extent which understanding is consistent with ground truth.
Consistency	Extent which understanding is consistent with relevant understanding at an earlier time period.
Currency	Time lag of understanding.
Precision	The level of granularity of understanding.
Contextual Attributes	
Completeness	Extent to which understanding necessary for decision making is obtained.
Accuracy	Appropriateness of precision of understanding for a particular use.
Relevance	Extent to which understanding is related to task at hand.
Timeliness	Extent to which currency of understanding is suitable to use.
Uncertainty	Subjective assessment of understanding uncertainty.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 109-110.

The third sub-component of individual sensemaking is the quality of individual decisions. It assesses how well an individual can use his awareness and understanding to make choices that are appropriate for the situation. Although decisions are context dependent, the quality of an individual's decisions can be assessed objectively over time. The quality of individual sensemaking is measured through the following attributes:

Table 9 – Quality of Individual Decisions Attributes

Objective Attributes	
Consistency	Extent which decisions are internally consistent with prior understanding and decisions.
Currency	Time taken to make a decision.
Precision	The level of granularity of decisions.
Contextual Attributes	
Appropriateness	Extent to which decisions are consistent with existing understanding, command intent, and values.
Completeness	Extent to which decisions encompass the necessary range of contingencies, breadth of force elements included, and time horizon.
Accuracy	Appropriateness of precision of decision for a particular use.
Relevance	Extent to which decision is significant to task at hand.
Timeliness	Extent to which currency of decision is suitable to its use.
Uncertainty	Subjective assessment of decision uncertainty.
Mode of Decision Making	Type of decision process utilized to make the decision.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 120-121.

Individual sensemaking can be compared to Carl von Clausewitz's concept of military genius; however two important distinctions stand out. First, NCO CF's concept of the quality of individual decisions does not account for *coup d'oeil* or the intellect of the individual to cut through the information to determine the truth of a situation.[22] Second, the NCO CF makes the distinction that individual sensemaking applies to all players in the collaborative decision making process and not just the genius commander leading the process.

[22] Carl von Clausewitz, *On War*. Edited and translated by Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1976), 102.

Degree of Shared Sensemaking Defined similarly to individual sensemaking, this concept measures the degree and consistency of awareness, understanding, and decisions across force entities. It uses the same attributes as the individual concepts shown in tables 7-9, but adds the objective attribute of extent to each in order to capture the pervasiveness of shared awareness, shared understanding, and collaborative decisions respectively. In other words, to what extent do forces sense, know, and decide on the same action with the information provided?

Quality of Interactions Laying at the intersection of the cognitive, social, and information domains, this key concept is a linchpin of complex and dynamic processes taking place inside the NCO CF. It takes stock of the human networking occurring in the social domain not only to share, but also to build information, awareness, and understanding and make decisions in pursuit of mission effectiveness. It goes beyond technology to assess how well individuals and organizations work together and use network-centric processes to share information and improve sensemaking. This concept assumes that "the characteristics and behaviors of organizations and individuals have an impact on the likelihood of successful interactions."[23] These characteristics can facilitate, be neutral, or derail collaborative decisions. For example, an organization's risk propensity, competence, trustworthiness, confidence, size, experience, permanence, and autonomy can all impact the quality of its interactions.[24] Organizational and individual behaviors may include extent of cooperation, efficiency of interaction, synchronization, and focus on the task at hand.[25] These characteristics and behaviors inform the following quality of interactions attributes:

---

[23] John Garstka, "NCO CF," ver 2.0 (draft), 134.
[24] John Garstka, "NCO CF," ver 2.0 (draft), 37.
[25] John Garstka, "NCO CF," ver 2.0 (draft), 139.

Table 10 – Quality of Interaction Attributes

Attributes	
Quantity	Amount of information, awareness, understanding, and/or decisions that are the focus of interactions.
Quality	Subjective assessment of the quality of interactions (voice, e-mail, chat, etc.).
Focus	Extent to which interactions focus on the task at hand versus team work.
Reach	The number of members that participate in the interactions.
Richness	The extent to which relevant and necessary participants collaborate.
Continuity	The persistence of the exchange among members (continuous or episodic).
Synchronicity	Type of interaction: synchronous or asynchronous in time and space.
Mode	Degree to which all senses are involved.
Latency	The time lag of interactions.
Agility	Subjective measure of robustness, resilience, flexibility, responsiveness, innovativeness, and adaptability.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 1.0, November 2003, 48 and John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 133.

Degree of Decision Synchronization Planned military actions can be conflicted, de-conflicted, or synchronized. Conflicted entities, plans, or expected actions work at cross purposes and actively interfere with the tasks of other entities. They are considered to analytically represent "the fog and friction of war."[26] De-conflicted entities are prevented from conflicting with one another by purposeful separation in time, or space, or both. Synchronized actions, like true combined arms actions, combine to make the whole greater than the sum of the parts. Synchronized actions are the goal and self-synchronized actions are the ultimate achievement of Network Centric Operational theory. This concept takes the output of the process to measure how well the plan

[26] John Garstka, "NCO CF," ver 2.0 (draft), 98.

has been communicated and shared throughout the force. In modern warfare, this decision must often be shared across numerous commands, echelons, countries, and times zones. Non-synchronized decisions are a sub-optimal condition which may hinder or prevent mission effectiveness. Specifically this concept measures the proportion of synchronized decisions compared to all decisions made. The metrics used to assess the proportion of decisions that are conflicted, de-conflicted, or synergistic are as follows:

1. The percentage of entities included in decisions that are conflicted, de-conflicted, or synergistic;

2. The percentage of plan elements that are conflicted, de-conflicted, or synergistic;

3. The percentage of expected actions that are conflicted, de-conflicted, or synergistic; and,

4. The percentage of time that decisions that are conflicted, de-conflicted, or synergistic.[27]

Degree of Actions/Entities Synchronized Building on the degree of decision synchronization, this concept moves out of the cognitive and social domains into the physical domain to assess how well the actions directed by collaborative decisions are synchronized. Stated differently, this concept determines whether the forces act in coordination. The concept represents the transition from the decisions made in the cognitive and social domains to the actions of the forces in the physical domain. It seeks to assess the proportion of actions and entities that are conflicted, de-conflicted, or synergistic through the use of the following metrics:

1. The percentage of entities categorized as conflicted, de-conflicted, or synergistic;

[27] John Garstka, "NCO CF," ver 2.0 (draft), 97-98.

2. The percentage of actions categorized as conflicted, de-conflicted, or synergistic; and,

3. The percentage of time that the force is classified as conflicted, de-conflicted, or synergistic.[28]

Degree of Effectiveness This concept assesses the results of the forces' actions to determine whether the actions accomplished the mission and the costs to do so. Typically used at the tactical or operational level, this concept measures the overall process in a manner useful for comparing different approaches to accomplishing the same mission. This concept can be directed toward three different measures of effectiveness, including Measures of C2 Effectiveness (MoCE), Measures of Force Effectiveness (MoFE), and Measures of Policy Effectiveness (MoPE).[29] When used to compare two different processes against each other, the differences in the attributes of effectiveness point to which process is better and by how much in terms of resources, time, or prestige. The following table describes the attributes of the effectiveness concept.

[28] John Garstka, "NCO CF," ver 2.0 (draft), 99.
[29] John Garstka, "NCO CF," ver 1.0, 21. The MoCE and MoFE measures of merit were developed by the Military Operations Research (MORS) community during the 1980s, while the MoPE measure of merit was developed by the NATO Studies and Analysis panel working group SAS-026 to account for the often conflicted or non-synergistic military and policy results. All three measures of merit have been incorporated into the *NATO Code of Best Practice for C2 Assessment* found here: http://www.dodccrp.org/files/NATO_COBP.pdf.

Table 11 – Attributes of Effectiveness

Attributes	
Achievement of Objectives	Degree to which strategic, political, military, economic, social, information, infrastructure objectives were achieved.
Agility	The degree to which force entities were robust, resilient, flexible, responsive, innovative, and adaptable.
Time	Time required to achieve objective.
Efficiency	Total cost of achieving objective.

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 100.

A rigorous analysis of the previous NCO CF concepts and attributes help explain why one warfighting organization is more effective than another.

Validation of the NCO CF

Cyberpower has demonstrated powerful capabilities to enable and enhance military action on the battlefield. The NCO CF was developed to explain how and why this is the case. The Secretary of Defense's Office of Force Transformation has conducted a number of studies to validate the NCO CF as an appropriate tool to help make procurement and doctrine decisions. Two case studies that use the NCO CF to illustrate the tenants of Network Centric Operations are examined below.

Link 16 Case Study

The first case study took an in-depth look at 12,000 F-15 training sorties. The results showed that pilots who were able to automatically share all radar information, including AWACS, through Link 16 data links increased their average day and night kill ratio by 2.6 times when compared to F-15s equipped with radios only.[30] The NCO CF explained and measured why this was the case.

With voice only interactions, the F-15 pilots must wait for the AWACS crew to form new radar tracks, see the new radar tracks,

[30] Daniel Gonzales et al., Link 16 Case Study, xxix.

understand what the new tracks mean, and notify the F-15 flight lead. Alternatively, Link 16 automatically sends the AWACS radar track to the F-15s so that both the flight lead and the wingman can see the enemy aircraft approaching and decide what to do in parallel with the AWACS crew. Figure 7 illustrates the difference between cuing and reacting to enemy aircraft entering into AWACS radar range for the flight lead and the wingman, with and without Link 16.

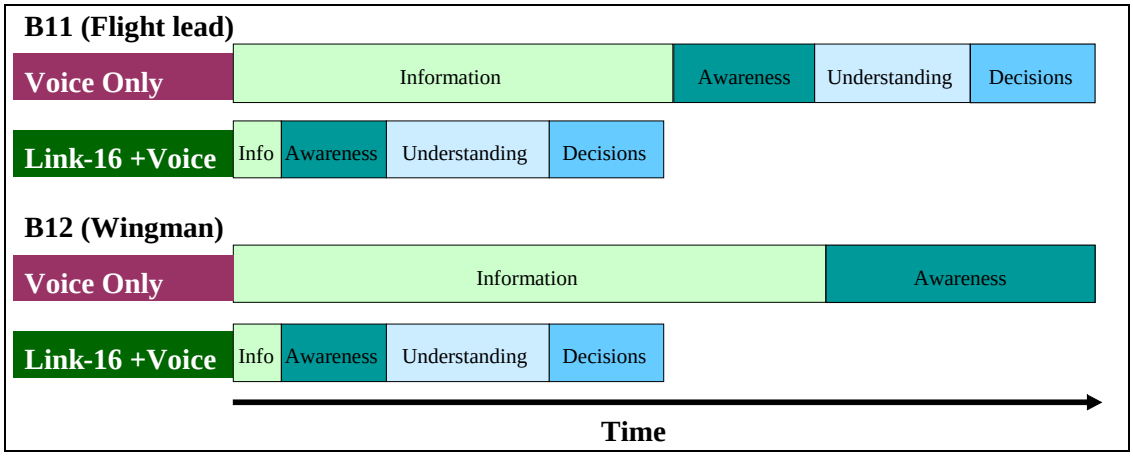


Figure 7 – Relative Comparisons of Decision Cycles With and Without Link 16
(Reprinted from John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 134)

Stepping through these scenarios, one can see the NCW tenets come to life. While both system configurations started with the same quality of organic information from the AWACS radar, the Link 16 network automatically shared that information with all parties, which increased the quality of shared information, which led to faster and improved sensemaking, resulting in effectiveness that diverged significantly between the voice only and voice plus link 16 systems. Figure 8 illustrates the difference between the Network Centric value chains of the F-15 with and without Link 16.

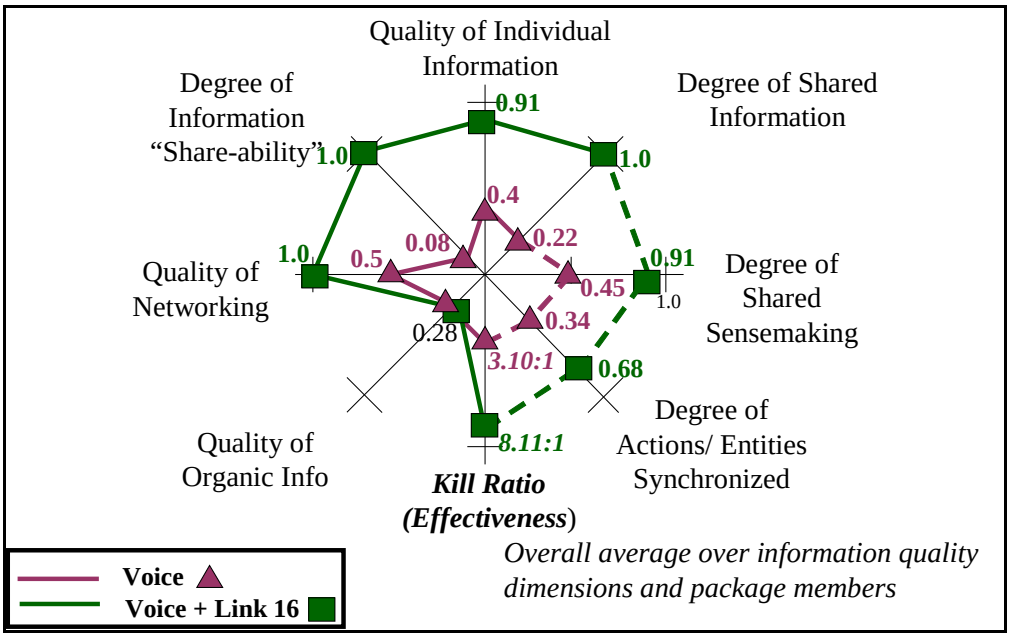


Figure 8 – Comparison of MCPs across Voice and Voice Plus Link 16 Systems
(Reprinted from John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 73)

Army Stryker Brigade Case Study

Rand's Army Stryker brigade case study provides an even more evocative example of the NCO tenets. The Stryker brigade was organized, trained and equipped around the robust networking, shared situational awareness, self-synchronization and speed of command concepts of Network Centric Warfare.[31] When pitted against a comparable Army standard light infantry brigade, the Stryker's closest predecessor, the Stryker brigade dramatically increased its mission effectiveness in an urban combat scenario as seen in the table 12.

[31] Daniel Gonzales et al., *Network Centric Operations Case Study: The Stryker Brigade Combat Team*, (Santa Monica, CA: RAND, 2005), xiv-xvi.

Table 12 – Comparison of Stryker Brigade and Light Infantry Brigade

	Light Infantry Brigade	Stryker Brigade
Quality of individual and shared information (enemy ID'd)	~10%	~80%
Speed of command (time to observe, orient, decide and make initial attack)	48 hours	3 hours
Blue : Red Casualty Ratio	10:1	1:1
Mission Success	No	Yes

Source: John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 105.

Compared to the traditional light infantry brigade, the Stryker brigade had new systems (C2, vehicles, and equipment), but more importantly a new operational concept, organizational structure, and networking capabilities.[32] The substitution of an embedded reconnaissance, surveillance, and target acquisition squadron for traditional infantry forces highlights just one of the ways NCO theory influenced the organization of the Stryker brigade. Together these capabilities enabled the Stryker brigade to better generate "its own situational awareness data and quickly fusing this data to generate high-quality situational awareness information and understanding."[33] The measures of effectiveness shown in table 12 highlight the real power of the NCO tenets.

Traditional Limits of the NCO CF

The authors of the NCO CF have maintained that it is a "work in progress," and indeed there are some limits to its current form.[34] David Alberts, John Garstka, and Frederick Stein proposed the tenets of Network Centric Operations in 1999, and the NCO CF built an analytical structure to explain and measure how its hypotheses hang together.

---

[32] Gonzales et al., Stryker Brigade Case Study, xiii.
[33] Gonzales et al., Stryker Brigade Case Study, xiii-xiv.
[34] John Garstka, "NCO CF," ver 1.0, 9.

However, the NCO CF is by definition conceptual and subject to change based on new information and propositions, the discovery of limiting conditions, or experimentation invalidating concepts and attributes. Despite the fact the model has not been fully adopted, the case studies above show that it can offer explanations in various contextual scenarios.

Further, while the model has broken the overall complexity involved in the process of gathering, distributing, and breaking information into component parts, complexities remain, albeit in smaller pieces. This compartmentalization can help researchers and executives focus development efforts, however the framework does not simplify the complexity of the cognitive and social aspects of entity interactions, sensemaking, and collaborative decisions.

Finally, the NCO CF is a neutral and descriptive assessment tool, not a prescriptive model. It is best used to analyze multiple scenarios in a specific context to determine which approach is better and why. It cannot specify what is needed to optimize net-centricity, nor does it spell out "how much is enough in terms of Network Centric technologies and practices." [35] The NCO CF, however, is a tool to help collect evidence and begin conducting the analysis needed to start answering such questions and points to areas for further research and development. Cyber warfare is one area that nations are clamoring to understand. Perhaps, applying the NCO CF to cyber engagements can bring further understanding.

Conclusion

Although, the world has not yet achieved a widespread conceptualization of the power of information, the NCO CF helps us take a few steps towards understanding how to utilize information's power during military operations. And even though the NCO CF has appreciable limits, it has already demonstrated analytical utility through a number of case studies. Since cyber-warfare is naturally a Network

[35] John Garstka, "NCO CF," ver 1.0, 9.

Centric Operation, it is worth considering whether the NCO CF can be applied to this type of warfare as well. Before determining whether the NCO CF can be applied to cyber engagements, one must understand how cyberspace engagements reflect differences from traditional military engagements that the NCO CF concepts may or may not be able to reconcile.

Chapter 2

The Cyber Differences That Matter

> *It is not information itself which is important but the architecture of and infrastructure for its collection, processing, and distribution which will be critical. Increasingly, advantage is achieved through investments in information systems, decision-making structures, and communication architectures.*
>
> Air Force 2025

Traditional Network Centric Operations studies focus on how useful cyberspace and human networking can be in traditional military operations. This thesis explores the possibility of applying the Network Centric Operations Conceptual Framework (NCO CF) to cyberspace engagements. Having explained the NCO CF in Chapter 1, this chapter examines the differences between cyberspace operations and traditional operations that will be important before attempting to apply the NCO CF to cyberspace.

Cyberspace represents the network within the NCO CF. However, delivering the benefits of cyberspace is not as straightforward as the NCO CF makes it appear. The NCO CF simplifies the cyberspace domain and does not address the duality of the real world cyberspace engagements that occur. In general terms, cyberspace engagements resemble a recursive, that is embedded, cyber-specific Network Centric Value chain inside the larger Network Centric Value chain. This embedded process has enemy forces that can impose or exploit the information in a cyberspace. The heart of this chapter strives to determine if a recursive application of the NCO CF to cyberspace is appropriate.

First Difference: Cyberspace is a Created Domain

Air, land, sea, and space do not exist, disappear, or change because of human interactions even though humans have created tools to exploit those domains. However, the cyberspace domain would not even exist without the effective interaction of manmade tools. Martin Libicki perhaps put it best when he said "cyberspace is built, not born."[1] Cyberspace, as defined in the introduction, only exists when two or more compatible nodes interact through the electromagnetic spectrum. The topology, capabilities, and attributes of a cyberspace are fundamentally defined by both the individual capabilities resident in the nodes and the interaction between the nodes. In other words, cyberspace operations necessitate the interaction of multiple compatible nodes, whereas military operations can occur when one person acts in the physical domains regardless of the capabilities of the target. Cyberspaces may also exist without human participation; once a human installs a particular node, the node can interact with compatible nodes without human direction. Furthermore, the physical interactions of cyberspace nodes occur through the rapid manipulation of the electromagnetic spectrum outside the range of human observation and understanding. Therefore, machines must modulate, interpret, and present these physical interactions so that humans can use them.

The domain grows increasingly complex as heterogeneous cyberspaces grow larger. Given the current state of technology, separate cyberspaces can be created with relative ease and private virtual cyberspaces can be created on the fly in "multiple, almost infinite, manifestations and forms" as desired.[2] However, once found and accessed, nodes or simple cyberspaces can also be easily denied or destroyed. Given their plug-and-play nature, these impaired nodes and

---

[1] Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, (New York, NY: Cambridge University Press, 2007), 5.
[2] Libicki, Conquest in Cyberspace, 5-6.

simple cyberspaces can usually be repaired with relative ease.[3] Creation, repair, and destruction become increasingly difficult as the size of the cyberspace grows. The amount of work required to create and repair a cyberspace increases in a linear fashion with an increase in the number of nodes. However, the network becomes more robust as more nodes and connections are added, thereby making denial and destruction of the entire cyberspace exponentially harder as the cyberspace grows in size and complexity.

Larger cyberspaces also necessarily give more opportunities for access to both intended and mischievous users. The modern Internet is the prime example of a large robust cyberspace. While it provides users access to heretofore unavailable capabilities, the Internet also highlights the less benign side of large cyberspaces, namely as access grows so do the opportunities for mischief.

These opportunities stem from the manipulation of flaws in the nodes and services available in a cyberspace. The National Institute for Standards and Technology addresses these concerns with a risk management approach. This approach defines risk as "a function of the likelihood of a given threat source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."[4] This definition is usually represented by the following equation: Risk = Vulnerability * Threat * Impact

Risk can theoretically be eliminated by reducing vulnerabilities, threats, or impacts to zero. This logic leads the information security community to opine, perhaps more than whimsically, the "most secure

---

[3] This point is conceptually similar to Martin Libicki's point that cyberspace is a replicable construct. He states that because cyberspace is replicable, it is also repairable. Libicki, *Conquest in Cyberspace*, 5.

[4] NIST, "Risk Management Guide for Information Technology Systems," Special Publication 800-30, 4.

application is one that is disconnected and locked in a safe."[5] In practice, without applying additional controls, any flaw in a node or service will increase the vulnerability, and thus the security risk to the system, as the size and access to the system increase. Information security professionals face the modern dilemma of balancing the tension between ubiquity and security. Initially, applications can be useful, but if they are not secure their utility can be turned against users. While it is inconceivable that a tank or airplane could be turned against the driver or pilot, cyberspace capabilities are commonly turned against their users.

As the creators of cyberspace capabilities, humans also create the rules for interacting inside a cyberspace. Summarizing this point Lawrence Lessig argued that "cyberspace has nearly no inherent properties and only a few strong tendencies; everything else is imposed by those with the power to do so."[6] Often this power accrues to those with the biggest base of users or those who control critical aspects of a cyberspace. Lynn White argued that "the acceptance or rejection of an invention, or the extent to which its implications are realized if it is accepted, depends quite as much upon the condition of a society, and upon the imagination of its leaders, as upon the nature of the technological item itself."[7] White's "condition of society" concept in cyberspace translates into installed user base and acceptance of the standards. Products with large numbers of users like Apple i-Tunes and i-Phone, Microsoft Windows, and the TCP-IP standard, and entities such as the Internet Corporation for Assigned Names and Numbers (ICANN) determine many of the rules of the Internet society. In their book

---

[5] Jesper Johansson, "Security Management – The Fundamental Tradeoffs," *Microsoft: Technet,* http://technet.microsoft.com/en-us/library/cc751266.aspx (accessed 7 May 2010).
[6] Quoted in Libicki, *Conquest in Cyberspace*, 7.
[7] Lynn White, *Medieval Technology and Social Change*, (New York, NY: Oxford University Press, 1966), 28.

Information Rules, Carl Shapiro and Hal Varian contend that economic principles of network externalities, switching costs, and marginal costs of production drive adoption and changes to the user base.[8] Recognizing this relationship they concluded that standards change the game from competing for a market to competition in a market.[9] Cyberspace differs from industrial business in that it also allows small sections of society, perhaps just one or two people, to thrive in their own way. These sub-groups can write their own rules to create tailored cyberspaces suited to their own individual purposes. These tailored cyberspaces may not accumulate a large user base because they go against White's condition of society and Shapiro and Varian's rules of information economics, however this misses the point. Tailored cyberspaces can be intentionally created to be proprietary or tightly controlled in order to make them more secure. Similar to security, uniqueness lies in tension with ubiquity.

The implications extending from this difference are quite large. Do you build out the network to increase overall value? Or do you purposefully keep the network small to reduce the information security risk? Should a new standard be imposed to make the system more secure, realizing that the value of the system may be decreased? The manifestation of these characteristics in modern networking technology, led the National Research Council to conclude: "Thus, cyberconflict is quite unlike the land, air, and maritime domains in which U.S. armed forces operate, and enduring unilateral dominance with respect to cyberconflict is not realistically achievable by the United States (or any other nation). This is not to say that the United States should refrain

[8] Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy,* (Boston, MA: Harvard Business School Press, 1999), 11-12, 13-14, and 16-17.
[9] Shapiro and Varian, *Information Rules,* 16-17.

from developing cyberattack capabilities—only that it should not expect enduring advantage from such development."[10]

Second Difference: Cyberspace Engagements Do Not Occur in the Physical Domain

John Perry Barlow, author of many Grateful Dead songs, said "Cyberspace is *un*real estate. Relationships are its geology."[11] Cyberspace engagements occur in the information, cognitive, and social domains, but not the physical domain. Unlike traditional military operations, where engagements involve movement and kinetic operations in the physical domain, cyberspace engagements never exit cyberspace. Direct actions in cyberspace can produce physical results, but they only do so to the extent that these physical entities are directly connected or controlled through a cyberspace.[12] Hostile cyberspace actions target an enemy's information to increase the aggressor's understanding of the enemy or deny the target its use of the information as intended.

Cyberspace engagements can be harder to comprehend than traditional military operations as they do not occur in the physical domain. This fact requires researchers to focus solely on the other domains of the NCO CF. These non-physical domains are not as well understood since military planners cannot directly interact with cyberspace nor observe cyberspace engagements. Unfortunately an individual's understanding is typically framed by direct observation.[13]

---

[10] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, editors, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, (Washington, DC: The National Academies Press, 2009), 39-40.

[11] John Perry Barlow, "The Next Economy of Ideas: Will copyright survive the Napster Bomb? Nope, but creativity will." *Wired*, October 2000, http://www.wired.com/wired/archive/8.10/download_pr.html (accessed 7 May 2010).

[12] Cyber engagements have demonstrated indirect physical effects – a significant caveat to this assertion. The most well known being the DHS sponsored Aurora Generator Test reported here: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (accessed 24 Mar 2010). While potentially significant, this type of attack is considered a niche area of cyber engagements since effects in the physical domain are highly dependent on the configuration and control of the target system.

[13] David Alberts et al, *Understanding Information Age Warfare*, (Washington, DC: Command and Control Research Program, 2001), 11.

The absence of this most reliable input makes the study and analysis of cyberspace perception and decision making all the more challenging. The NATO Research and Technology Organization summarized this challenge in the following excerpt:

> The focus of military research and analysis has predominantly been on the physical domain. C2 [Command and Control] deals with distributed teams of humans operating under stress and in a variety of other operating conditions. C2 problems are thus dominated by their information, behavioral, and cognitive aspects, which have been less well researched and understood. This focus creates a multidimensional, complex analytic space that involves multi-sided dynamics including friendly, adversary, and other actors, action reaction dynamics, and tightly coupled interactions among elements such as doctrine, concepts of operations, training, materiel, and personnel.[14]

As a result, when the physical domain has been removed from consideration, the analysis of cyberspace is more difficult.

Information created and stored in a cyberspace represents the prime resource of the domain. As with natural resources in the physical domain, information can be used to build wealth and power. Like the physical domain, adversaries compete intensely over these information resources; competition that frequently leads to conflict. Unlike the physical domain, however, information cannot be consumed and can be quickly copied and transported multiple times for little or no cost. Creating cyberspaces facilitates the competition for information; therefore important information must be protected and secured in order to keep secrets.

Third Difference: Stealth

While militaries have tried to escape detection for centuries, offensive cyberspace engagements require surprise and stealth. Cyber exploits and attacks, once observed, typically can be quickly blocked and

[14] "NATO Code of Best Practice for C2 Assessment: Analyst's Summary Guide," http://www.dodccrp.org/events/12th_ICCRTS/CD/library/html/pdf/NATO_Analyst.PDF *(accessed 24 Mar 2010), 3.*

any resulting damage repaired in short order because cyberspace is a created domain.

Stealth in cyberspace can be gained by manipulating a flaw, hiding in a large volume of communications, hiding amongst the complexity of a cyberspace, or through a combination of all three. Flaws in programs, devices, or configurations allow attacks to seem like innocuous activity to users, administrators, and sensors. Given the high volume of traffic in most cyberspaces, an attack, even if it would be identified on its own, can get lost in the high volume of traffic and other anomalies occurring at the same time in an "exponentially growing volume of digital traffic."[15] For cyberspace security professionals sometimes it's like looking for needles in a fast moving conveyor of haystacks. Finally, cyberspace can be so complex that opportunists can achieve stealth by hiding in plain view. For example, an installation team could misconfigure a wireless network server, allowing access to an otherwise secure network.

When successful, stealthy cyber exploits will completely bypass the cognitive, information, and social domains of an opponent. The target cyberspace cannot sense the exploit, does not generate organic information on it, and therefore has no information to share, understand, or use for decision-making. The key to defending against stealthy exploits is to enhance the NCO CF concept of individual and shared understanding by developing and monitoring sensors to feed new types of organic information to friendly forces. Cyber attacks would therefore be more obvious because their effects can be observed. Once an attack changes or blocks data, security professionals can account for those changes by using the NCO CF consistency attribute which measures the "extent to which information is consistent with previous versions."[16]

---

[15] David Fulghum, "Cyber-Warriors Begin Training," *Aviation Week*, 29 Mar 2010, 48, http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?storyID=news/awst_032910_p48.xml&headLine=null (accessed 31 March 2010).
[16] John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 110.

Fourth Difference: Speed of Interactions

In traditional military operations, actions go no faster than the quickest vehicle. The fastest of these are bullets, missiles, and jets that take seconds, minutes, or hours to get to their destinations. With many of these types of attacks, sensors can give those on the receiving end time to react. Cyberspace engagements, on the other hand, happen at computing speeds delivered at the speed of light. Once these engagements start, even if observed, they occur much faster than humans can react. As a result, the targets of cyberspace attacks typically can only make adjustments (e.g. strengthen their defenses and remediate damage) after an attack is completed. While total security will likely never be achievable, network defenders can improve their performance by creating automated response tools.

Automated cyber defenses fall into two categories: reactive Intrusion Detection Systems (IDS) and proactive Intrusion Prevention Systems (IPS). IDS automate "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."[17] Einstein II, perhaps the best known network-based IDS, is designed to enable analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology."[18] IDS provide a half measure toward automating engagements in cyberspace. These systems can sense

---

[17] National Institute of Standards and Technology Special Publication 800-94, "Guide to Intrusion Detection and Protection Systems," (Gaithersburg, MD: NIST, Feb 2007), 2-1, http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (accessed 24 March 2010).

[18] National Security Council, "The Comprehensive National Cybersecurity Initiative," http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 29 May 2010).

attacks and notify network defenders, but do not automatically take measures to limit the damage of an offensive action. Network defenders using an IDS can, at best, prevent further damage.

IPS takes the IDS concept one step further in its ability to respond to detected incidents. An IPS conducts all of the activities of an IDS and automates "attempt(s) to stop possible incidents."[19] Current research on these systems is focusing on heuristics used to detect an attack in the ocean of normal traffic and take appropriate steps to mitigate the offensive action without negatively impacting legitimate user traffic. The operational prototype Einstein III IPS has been likened to an "anti-aircraft weapon, (able to) shoot down an attack before it hits its target."[20] If a cyberspace has unknown flaws, and all systems potentially have unknown flaws, automated IPS offers one of the only ways to protect against them before they are exploited.

Fifth Difference: Surprise or Perishability of Advantage

Since the beginning of time, enemies have reacted to the introduction of new weapons, tactics, and doctrine with countermeasures of their own. The introduction of new countermeasures starts with the theory, or more typically the surprised observation, of a new weapon, tactic, or doctrine. Over time, responses are theorized, developed, and rolled out in response to enemy action. There are dramatic differences in how this action-counteraction cycle occurs across the physical domain and cyberspace.

In the traditional physical domain, countermeasures to new weapons may partially or completely negate the advantage the new weapon, tactic, or doctrine provided the enemy. For example, German anti-aircraft guns successfully countered allied bombing by partially negating its overall effectiveness. However, not only did this

---

[19] National Institute of Standards and Technology Special Publication 800-94, 2-1.
[20] CNN, "Homeland Security Seeks Cyber Counterattack System," *CNN.com/technology*, 4 Oct 2008, http://www.cnn.com/2008/TECH/10/04/chertoff.cyber.security/ (accessed 24 March 2010).

countermeasure take time to develop and roll out across Germany, but it did not completely eliminate the threat of the bombers. The Germans, furthermore, dedicated a tremendous amount of resources to manufacture and man anti-aircraft systems to eventually show such partial results. These resources necessarily took away from Germany's overall war effort.

An attack or exploit in cyberspace, necessarily takes advantage of an unknown vulnerability. Once an attack is discovered and understood, it may become immediately ineffective. Countermeasures that completely eliminate a vulnerability can be quickly developed and automatically deployed across the enterprise. As a result, the attack, even if originally highly effective, can be completely countered without continuing to use additional resources to prevent its future use. On the other side of the coin, if an attack or exploit is not used, the targets may eliminate the vulnerability before the attack is ever launched.

This difference makes it difficult to evaluate the potential efficacy of offensive action in cyberspace since an attack or exploit that is effective one day may become ineffective the next. Any conceivable offensive action that shows promise in tests can have three possible outcomes. It may not work at all. It may work and not be observed, thus retaining utility for future action. Or it may work one time, but be quickly, totally, and permanently countered.

Sixth Difference: Internet is a Mix of Commercial, Private and Government Interests

While the NCO CF does not necessarily exclude the interaction of non-military entities, the Internet, representing the world's largest and primary cyberspace, is a heterogeneous mix of organizations that require consideration. The architecture of cyberspace does not make the nature

of the activity nor the responsible party apparent.[21] Therefore, it may not be obvious whether observed malicious cyberspace activity is an act of war, an act of terrorism, or a criminal activity.[22]

This situation necessitates close interaction between military, law enforcement, and private industry in order to respond appropriately. This interaction requires collaboration beyond military and political channels of the executive branch. This is exactly like the collaboration suggested in the NCO CF, however this private-public-federal-state interaction results in an environment much more complex than traditional military operations.

Conclusion

When looking through the lens of the NCO CF, the six differences highlighted above represent the key distinctions between traditional military operations transpiring in the physical domain and cyber operations occurring largely in the information domain. While there are other differences such as reach, costs, economic profits, and sovereignty that can impact the use of cyberspace engagements, these difference are less of a concern with respect to the NCO CF.

In light of the differences outlined above, one can conclude that the NCO CF must at least be modified before it can be applied to cyberspace engagements. Before suggesting what modifications could be made to the NCO CF, one needs to understand the nature of cyberspace engagements.

---

[21] Susan Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, (New York, NY: Oxford University Press, 2009), 9.
[22] Brenner, *Cyberthreats*, 9.

Chapter 3

Candidate Cyberspace Engagement Model

…when the paradoxical logic of strategy assumes a dynamic form, it becomes the coming together, even the reversal, of opposites.

Edward Luttwak in Strategy: The Logic of War and Peace

An armed attack against one [NATO alliance member] shall be considered an attack against them all.

NATO Article 5

As outlined in the previous chapter, traditional military operations differ significantly from military operations in cyberspace. Indeed, these ethereal and at times paradoxical differences tend to obfuscate the realities of cyberspace and make it difficult to analyze using traditional methods. In light of these differences, this chapter proposes a candidate cyberspace engagement model to understand and analyze cyberspace engagements by laying out the key components and concepts of cyberspace engagements.

Candidate Cyberspace Engagement Model

A cyberspace is created to provide a utility that is "exponentially greater than the cost."[1] The private, public, and military sectors have derived so much utility from their cyberspaces that many have declared an information-based revolution in each sector.[2] Alvin and Heidi Toffler posited that this utility is providing such broad, deep, and profound benefits that it is revolutionizing the entire society into a "Third Wave" of

[1] Sam Liles, "Into the Darkness of Cyberspace," Selil.com, posted on 9 Mar 2009, http://selil.com/?p=645 (accessed 15 Dec 09).

[2] This information revolution takes many forms in current literature. Alternatively called post-industrial, knowledge-based, new-economy, internet-economy, etc in the economy. Similarly, it has been called e-government or government 2.0 in the government and Revolution in Military Affairs (RMA) for the military.

transformation.[3] Like the first wave of agricultural changes and the second wave of industrial changes, the information wave is sweeping the military up with it. As the military transforms itself in the information age, its effectiveness and "power [are] increasingly derived from information sharing, information access, and speed, all of which are facilitated by networked forces."[4] Warfare is a contest of wills, however, so no one should assume the method and tools for utilizing information will be uncontested. One need look no further than Sun Tzu's spies or the Allied breaking of Germany's enigma codes during World War II to see that this is not a new concept. Cyberspace is bound to be used in the same cunning and devious ways that adversaries have historically resorted to in warfare in other domains.

Although the military creates useful cyberspace tools, these tools frequently contain inherent, unintended, and unknown flaws which create vulnerabilities in the physical or syntactic layers of a cyberspace.[5] This is the central dilemma of cyberpower discussed in the previous chapter. Cyberspace aggressors, once they have discovered such vulnerabilities, can surprise their target to exploit the vulnerability to steal information or attack them to disrupt, deny, degrade, or destroy information and utility. After the intended users realize that a cyberspace has been attacked or exploited, they will understandably take defensive measures to protect the cyberspace's utility. The dynamic interaction of creating, operating, attacking, exploiting, and defending activities in cyberspace represent the operational categories of today's

---

[3] Alvin and Heidi Toffler's forward to Arquilla, John and David Ronfeldt's book, *In Athena's Camp: Preparing for Conflict in the Information Age*. (Santa Monica, CA: Rand, 1997), xiii-xiv.

[4] Director, Force Transformation, Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, (Washington, DC: DOD, 2005), i.

[5] Vulnerabilities can also intentionally created by the software or hardware developers. While this is a real and growing concern, they will be treated in the same category as unintentional and unknown vulnerabilities.

cyberspace hostilities. The Candidate Cyberspace Engagement Model describes these categories and their dynamic interactions below.

Creating Cyberspace Capabilities

Since cyberspace is a man-made domain, the candidate model begins with the creation of cyberspace tools that take advantage of cyberspace's network characteristics. Creation can be understood conceptually as the building or programming of a cyberspace tool that adheres to the requirements of the physical, syntactic and semantic layers to create potential utility for the user. This capability can be embedded into hardware, coded as firmware, or programmed as software. For a tool to provide cyberspace capability, it must be installed and operational in at least one node and connected to at least one other node.[6] Use of the tool then provides users new capabilities (e.g. web surfing, chat, virtual collaboration, dynamic mapping, etc.). For cyberspace capabilities, like e-mail, the utility of the tool to each user increases exponentially as the number of people using the tool increases. This increase has been described as Metcalfe's law, which proposes that the value of the network is proportional to the square of the number of connected users.[7] Metcalfe's law is an important characteristic of cyberspaces.

The Candidate Cyberspace Engagement Model incorporates a generic schema to aid understanding. The first portion of this schema labels each cyberspace capability with a different tracking number. For example, tools like Microsoft Word, Adobe Acrobat, and Cisco Internetwork Operating System would each be given a different tracking number. This number keeps individual utilities distinct from one

---

[6] This definition necessarily excludes capabilities on standalone machines. While standalone capabilities may be important for accomplishing certain tasks, they do not benefit from access to other users in a cyberspace. As such, they are excluded from further analysis in this paper.

[7] Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law is Wrong," IEEE Spectrum, July 2006, http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong (accessed 29 May 2010) .

another, but the schema uses a simple and consistent method for doing so. Importantly, distinct physical, syntactic, or semantic capabilities are given different tracking numbers. All cyberspace capabilities do not need to be tracked in this manner, but it helps to consistently track those capabilities that can be attacked. Since it is difficult to know whether a cyberspace capability can be attacked ahead of time, it makes sense to systematically track all cyberspace capabilities.

The second portion of the schema assigns a version number to each cyberspace capability. Version numbers, similar to software version numbers, would increase with each capability upgrade or modification (e.g. cyber capability X progressing from version X.0, X.1, X.2…).[8] Cyberspace security personnel need to distinguish between capability versions since new versions could eliminate specific vulnerabilities, but also introduce new ones. Tracking cyberspace capabilities in this way would make it easier to track a capability from the time it was created and subsequently attacked and defended. Figure 9 represents version N of a single cyberspace capability C.

Figure 9 – Cyberspace Capability C version N
(Source: author's original work with assistance from Mr. John Garstka)

Extending the illustration of a model cyberspace shown in Figure 2, cyberspace capability C.N above uses the potential utility of a single node to interact with other nodes in the cyberspace. Often hundreds of network capabilities populate each node, while an individual cyberspace can include thousands of nodes with a unique mix of network capabilities and versions at each node.

[8] Additional sub-versioning of cyberspace utilities is certainly possible, and if implemented would likely be beneficial. For purposes of conceptual understanding, sub-versioning is not considered further in this paper.

Creating Cyberspace Vulnerabilities

Creating cyberspace capabilities runs the risk of simultaneously creating vulnerabilities that cyberspace aggressors can manipulate and exploit. Why is this true? There are three broad categories of vulnerabilities: inherent, unintentional, and intentional. Inherent vulnerabilities are derived from the nature of the capability. For example, cyberspaces that use radio transmissions are vulnerable to jamming due to the inherent properties of radio signal propagation. Unintentional vulnerabilities exist because cyberspace capabilities may contain flaws. Flaws offer aggressors potential avenues of attack and exploitation when such capabilities are used within a cyberspace. These avenues of attack may be used to attack or exploit the capability directly or, more importantly, to establish a toehold and gain access to other capabilities, flaws, parts, users, and information in a cyberspace. Flaws can also be exploited to create hidden and remote access workarounds that can be reliably used in the future, even after a flaw has been repaired. Intentional vulnerabilities, often called backdoors, are surreptitiously built into cyberspace capabilities to allow the creator and collaborators to bypass the security measures of unsuspecting users. From the perspective of the intended user, these three types of vulnerabilities can be either known or unknown.

Types of Cyberspace Capabilities

With the concepts of cyberspace capabilities and vulnerabilities in hand, the six different types of cyberspace capabilities in the candidate model can be enumerated. These capability types cover the gamut of functionality, from providing network services as the Internet was originally intended, to operating and controlling those services across large cyberspaces, to attacking and exploiting vulnerabilities in a cyberspace, defending a cyberspace from attack, and building an awareness of activities inside a cyberspace. Figure 10 shows the different types of cyberspace capabilities graphically:

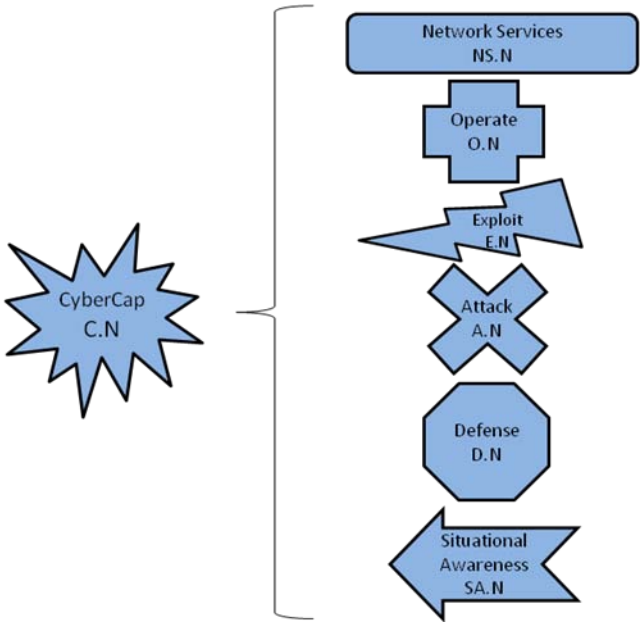


Figure 10 – Six Types of Cyberspace Capabilities
(Source: author's original work with assistance from Mr. John Garstka)

Each capability type uses the same numbering scheme described for generic cyberspace capabilities, but breaks them into six separate lists. The six capability type in this schema will be used throughout this thesis and are described below.

Network Services Network service capabilities describe the tools used to provide basic cyberspace utility. Using these capabilities to achieve enhanced military operations are the primary mission of a cyberspace. It may include things like e-mail applications, web browsers, database programs, video games, online collaboration, and remote access tools.[9] Most cyberspace capabilities fall within this category and it is often the only capability type considered by cyberspace users.

[9] There may be confusion in this terminology since many of these capabilities are often called Core Services by DISA and in Service Oriented Architecture literature. However, the definition of Network Service in this thesis applies to all capabilities and is necessarily larger than the small set of core services offered by DISA and SOA (SMS, messaging, search, storage, authentication, collaboration, etc.).

Operation Capabilities Cyberspace operation capabilities are required to support, deliver, and control the delivery of network services across a large enterprise. These capabilities provide "integrated network visibility and end-to-end management of networks, global applications, and services across the Global Information Grid."[10] At the tactical level these capabilities allow cyberspace system administrators to create, configure, and remove cyberspace capabilities, user accounts, and permissions throughout a cyberspace. Likewise "network visibility enables commanders to manage their networks as they would other combat systems."[11] Tools that fall into this category include identity management programs, policy management, network control, and storage management.

Attack and Exploitation Capabilities As mentioned previously, cyberspace attack and exploitation capabilities take advantage of inherent, unintentional, and intentional vulnerabilities in cyberspace. The Department of Defense has recognized the importance of these capabilities, labeling them Computer Network Attack and Computer Network Exploitation. Information Operations doctrine defines these terms as follows:

> Computer Network Attack (CNA)—Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
>
> Computer Network Exploitation (CNE)—Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.[12]

---

[10] Joint Chiefs of Staff, "Joint Publication 6-0, Joint Communications System," 20 March 2006, IV-1, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf (accessed 6 April 2010).
[11] Joint Chiefs of Staff, "Joint Publication 6-0," IV-1.
[12] References for CNA, CNE & CND are taken from Joint Chiefs of Staff, "Joint Publication 3-13, Information Operations," 13 February 2006, *GL-5 - GL-6,* http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 29 Mar 2010).

Three requirements must be satisfied to attack or exploit a vulnerability: discovery of the vulnerability, knowledge of how to attack or exploit the vulnerability, and access to the targeted node. If cyberspace aggressors can meet all three conditions, they can compromise the utility of that cyberspace.

Returning to the schema of the candidate model, when generic network service NS.N is created and deployed it may contain many different vulnerabilities. Cyberspace aggressors may develop attack or exploit capabilities that take advantage of these vulnerabilities. The Candidate Cyberspace Engagement Model schema categorizes attack and exploitation capabilities in the same manner as cyberspace capabilities, namely attack or exploitation number followed by a version. As an example, consider the newly created and deployed cyberspace utility NS.N. If there are two techniques that can be used to attack vulnerabilities of NS.N they would be cataloged as attack capability A version 0 and attack capability A+1 version 0.

No one-to-one relationship exists between capabilities, vulnerabilities, and attacks. A single capability may contain a number of vulnerabilities; each vulnerability may offer a number of avenues for attack; and, attacks can work against multiple vulnerabilities. To illustrate this point, consider a software application that is deployed over the Internet, like Google Documents. This capability may be susceptible to denial of service attacks at the source (Google) or destination (user), it may have weak security that allows aggressors to bypass encryption techniques to view or change the content, and it may transmit potentially sensitive information in a way that can be intercepted. The same vulnerabilities may also be found in a number of different applications, which would allow the same attack or exploit to be used against numerous applications.

Similar to creating a network service capability, creating an attack capability provides potential utility to the aggressor. From the

perspective of the cyberspace aggressor, an attack capability only becomes useful when it has access to the cyberspace capability containing the vulnerability. This observation can be considered the dark side of Metcalfe's law. For a normal network service capability, the greater the number of users and nodes, the greater the utility. However, if the widely used capability includes a vulnerability, the greater number of users also makes it easier for the aggressor to achieve the third requirement for offensive action—access to the nodes containing the vulnerability. Additionally, large cyberspaces generally offer a bigger target to attack with a greater amount of information to exploit.

Security professionals have discovered thousands of attacks and exploits. Top exploitation capabilities include phishing e-mails, websites containing malicious code which exploits the computers of visitors, and causing operating systems to fail in a ways advantageous to the aggressor.[13] By and large, cyberspace attacks use similar techniques as exploits, but their goal is to alter or prevent the use of information rather than just copying information during exploitation. However, jamming type attacks use techniques not found in the exploiter's toolkit. The most common jamming attack on the Internet is the Distributed Denial of Service attack and it has achieved limited success against a number of company and government websites.[14]

Cyberspace Defense Cyberspace defense capabilities endeavor to protect cyberspaces from exploitation and attack. The Department of Defense defines Computer Network Defense as follows:

> Computer Network Defense (CND)—Actions taken to protect, monitor, analyze, detect and respond to unauthorized

[13] SANS, "Top Cyber Security Risks," Sep 2009, http://www.sans.org/top-cyber-security-risks/ (accessed 29 Mar 2010).
[14] CERT Coordination Center, "Denial of Service Attacks," 4 June 2001, http://www.cert.org/tech_tips/denial_of_service.html (accessed 30 May 2010).

activity within Department of Defense information systems and computer networks.[15]

Once defenders identify a vulnerability, they must develop and deploy defensive techniques to block, prevent, or otherwise diminish the utility of an attack against the vulnerability.[16] Usually cyberspace defenders cannot identify a vulnerability until after they catch an aggressor exploiting it. One can understand this dynamic interaction between offensive and defensive actions through the candidate model. Using the candidate model schema, once cyberspace defenders discover a notional attack capability A.N, defenders will create D.N or upgrade to D.N+1 to mitigate the vulnerability and inform the creators of NS.N to patch the program and subsequently install NS.N+1 to remove the vulnerability. Since most large cyberspaces deploy a defense-in-depth concept, network defenders will probably deploy a number of defensive capabilities when a vulnerability is discovered.

Situational Awareness Situational Awareness capabilities are those tools and programs that monitor activity in a cyberspace for malicious activity. These tools aim to "gain an understanding of what is happening around a specified domain."[17] These capabilities attempt to lift some of the fog of cyberspace to identify malicious activity as it is occurring, to curtail negative impacts, and collect forensic evidence after an attack. "Situational awareness combined with proper risk assessments, including intelligence loss or gain determinations, allows

---

[15] References for CNA, CNE & CND are taken from Joint Chiefs of Staff, "Joint Publication 3-13," GL-5.

[16] Defenders may choose to leave vulnerabilities exposed in order to take advantage of the aggressors. Such efforts, often called honey pots, can snare the aggressor to feed false information, determine their identity, catalog attack and following techniques and signatures, or respond in kind.

[17] Kevin Coleman, "Cyber Situational Awareness," *Defensetech*, http://defensetech.org/2010/01/18/cyber-situational-awareness/ (accessed 29 March 2010).

commanders to make the best decisions on courses of action."[18] In other words, Situational Awareness tools attempt to build awareness for cyberspace defenders in the information and cognitive domains so they increase the chances of finding stealthy attacks and exploitations.

Situational awareness tools follow the same schema proposed above and are labeled generically as SA.N. Examples of situational awareness tools include Lookingglass' ScoutVision,[19] Symantec's Cyber Threat Analysis Program,[20] and ACSI's CyberSA.[21] All of these products attempt to fuse information from scanners, firewalls, sensors, and other equipment to provide the cyberspace defender with in-depth knowledge of what's wrong or odd, what it means, what's going to happen next, and what can be done about it.[22]

Basic Cyberspace Engagement Scenarios

The schema outline above can help one conceptualize and understand the interactive nature of the contest of wills between creation, exploitation, attack, and defense. Once a cyberspace attack or exploit is launched, three basic scenarios can unfold: 1) The defense succeeds and the offensive action is thwarted, 2) The offensive action is successful and not detected, or 3) The offensive action is successful, but detected. Appendix A shows the details of these three scenarios graphically.

---

[18] Donald Rumsfeld, "National Military Strategy for Cyberspace Operations," 11 Dec 2005, 17, http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 6 April 2010).
[19] Lookingglass, "Scoutvision: The Industry's Most Reliable and Intuitive Cyber Intelligence Platform," http://www.lgscout.com/products/scoutvision (accessed 29 March 2010).
[20] Symantec, "Symantec Utilizes Security Intelligence and Experts ti Deliver Cyber Threat Analysis Program," 28 Jul 2009, http://www.symantec.com/about/news/release/article.jsp?prid=20090728_01 (accessed 29 March 2010).
[21] Adaptive Cyber Security Instruments, Inc., "Stopping the Unstoppable – Your Best Line of Defense," http://www.acsi-cybersa.com/Products.html (accessed 29 March 2010).
[22] Jason Li and Peng Liu, "Bayesian Security Analysis: Opportunities and Challenges" presentation to the ARO Workshop, 14 Nov 2007, slide 5, http://ist.psu.edu/s2/ARO-SA/ (accessed 29 March 2010).

Proper feedback can improve cyberspace capabilities in the first and third scenarios. In the first scenario, this feedback would help the aggressor improve its attack and exploitation capabilities. In scenario three, cyberspace defenders who observe an attack or exploit occurring should inform the next version or upgrade of the target's network service and defense capabilities.[23] If an attack or exploit is detected, steps must be taken to thwart future occurrences. An effective upgrade would eliminate the capability of the attack or exploit from doing further damage and change the situation to scenario one. Scenario two is the most problematic for cyberspace defenders since the attack or exploit is not observed. As such, it can also be the most dangerous for those using cyberspace for its intended purposes since they could be unwittingly providing information directly to their enemies. The remaining NCO CF analysis will focus upon improving CND in the second and third scenarios.

Synthesis of Vulnerabilities and Capabilities Combining the concepts of vulnerabilities with capabilities highlights an important insight. The logic is as follows: since all cyberspace capabilities are created and all creations may be created with flaws, all creations contain flaws. Since humans create all six types of cyberspace capabilities, they can all have vulnerabilities. This concept is represented in Figure 11 below:

[23] Maintenance and normal user feedback also inform the creation of the next iteration, but are not included in this analysis since these users are not likely malicious.

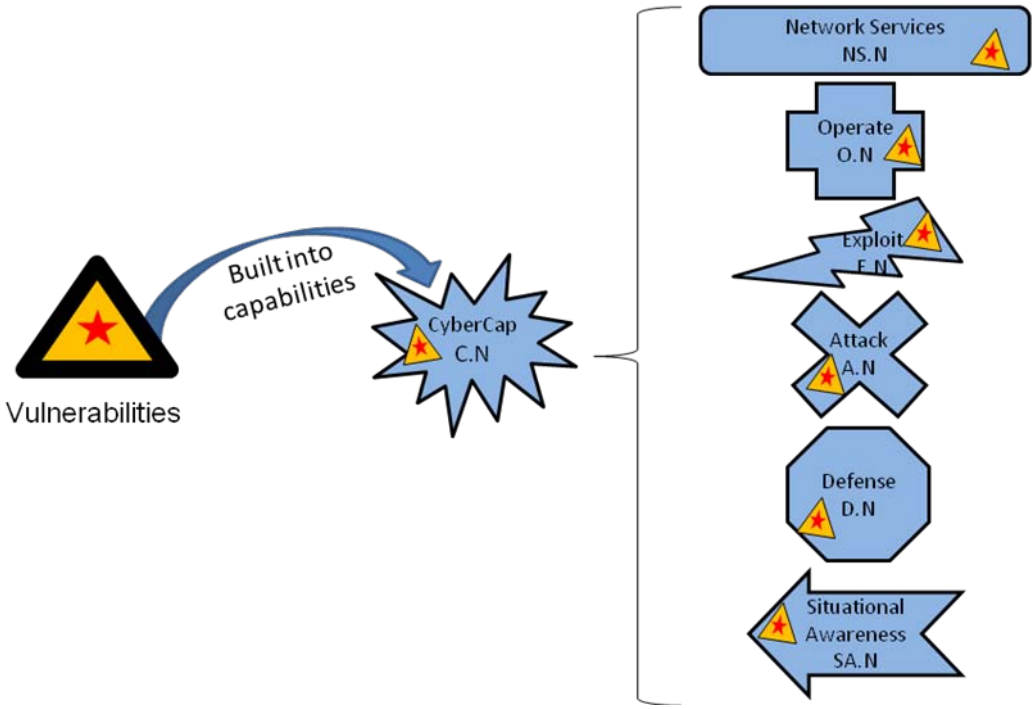


Figure 11 – Vulnerabilities Can Exist in All Cyberspace Capabilities
(Source: author's original work with assistance from Mr. John Garstka)

Some interesting defense scenarios flow from this synthesis. For example, an attack could theoretically target a vulnerability in situational awareness or defense capabilities to facilitate or hide future attacks. Such a move would give the aggressor virtual and perhaps indefinite carte blanche access to the target cyberspace. Alternatively, one could exploit flaws in an aggressor's attack or exploitation capabilities. This has the theoretical potential to compromise the utility of the attack or exploitation capabilities or potentially provide backdoor access to an aggressor's cyberspace. Many more combinations are certainly possible.

Using this synthesis, the basic cyberspace engagement scenarios described above can be extended. Figure 12 expands the simplified view of scenario three (a successful but observed attack). It is a more complete version of scenario three and represents the typical steps of a military-against-military cyberspace engagement.

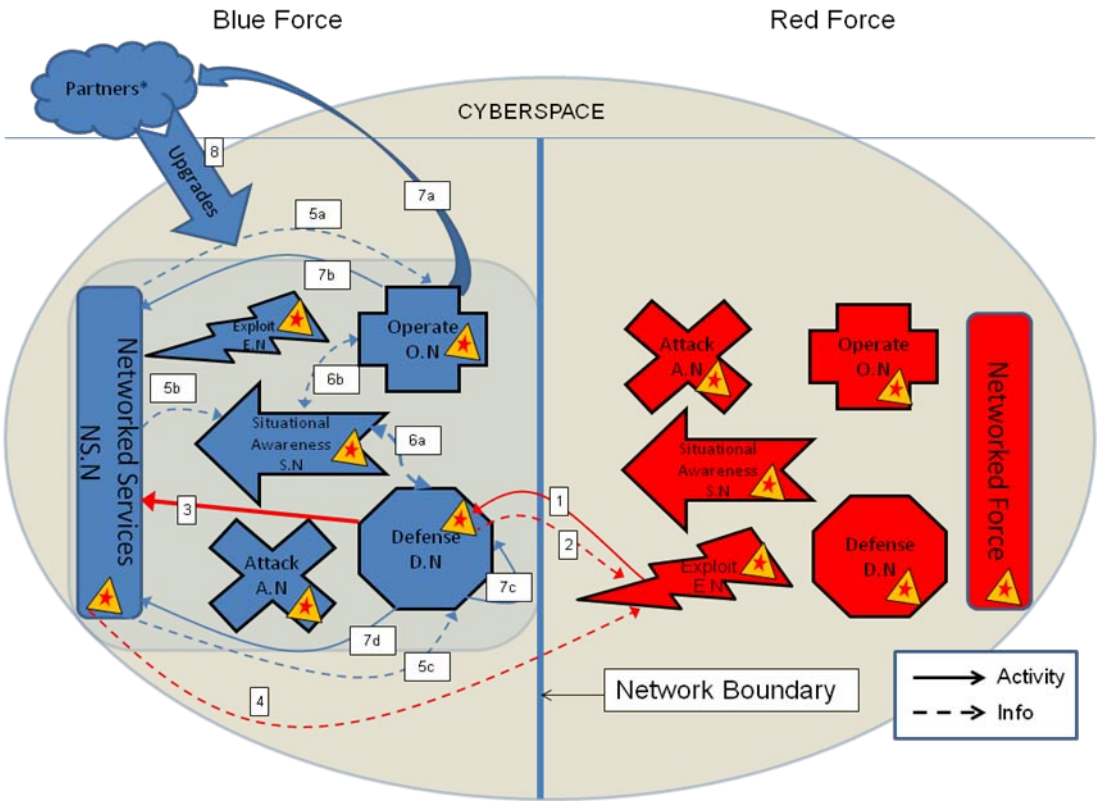


Figure 12: Extended View: Typical Cyberspace Engagement--Successful, but Observed Exploit

(Source: author's original work with assistance from Mr. John Garstka)

Note – Steps with multiple entries happen concurrently

Step 1 – Red Force launches exploit capability E.N

Step 2 – Red Force explores Blue Force's cyberspace to find additional vulnerabilities to exploit

Step 3 – Red Force exploits vulnerability in networked services capability NS.N to find information

Step 4 – Red Force begins extracting information from networked services NS.N

Step 5a – Operation capability O.N observes an anomaly in NS.N

Step 5b – Situational awareness capability SA.N detects Red Force Exploit Capability E.N

Step 5c – Defense capability D.N receives an alert from Networked Service NS.N

Step 6a – Defense capability agents collaborate with Situational Awareness capability agents to determine way ahead

Step 6b – Operation capability agents collaborate with Situational Awareness capability agents to determine way ahead

Step 7a – Operation capability agents collaborate with developers to upgrade capabilities to successfully defend against red force exploit E.N

Step 7b – Operation capability agents make configuration changes (as applicable) to Networked Services NS.N to negate the effectiveness of red force exploit E.N

Step 7c – Defense capability agents make configuration changes (as applicable) to Defense capability D.N to protect against red force exploit E.N

Step 7d – Defense capability agents make configuration changes (as applicable) to Networked Service capability NS.N to protect against red force exploit E.N

Step 8 – Allied, government, and industry partners provide upgrades, new capabilities or suggest configuration changes to the Blue Force cyberspace.

Cyberspace analysts can use the extended model above to conceptualize the interaction of thousands of software versions, millions of users, large numbers of partners, and numerous enemies in cyberspace. This extension can be visualized in Figure 13 below:

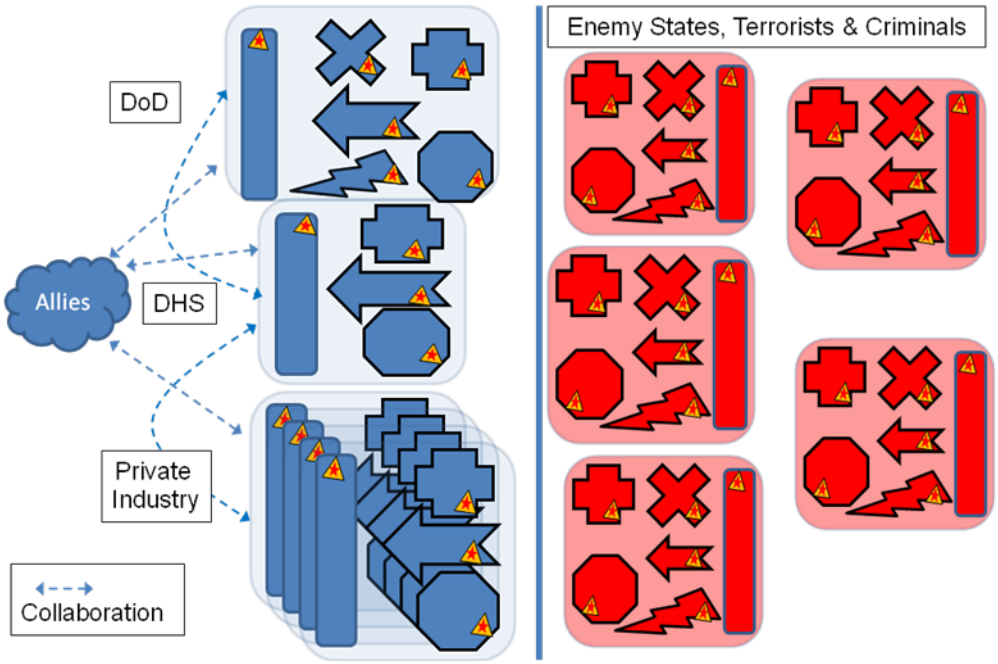


Figure 13 – Macro View of Government, Allied, Commercial and Enemy Forces
(Source: author's original work with assistance from Mr. John Garstka)

Limitation of the Candidate Model

Cyberspace's speed of interactions remains the lone difference that cannot be accounted for directly in the candidate model. One can say, quite correctly, that the goal of cyberspace defenders should be to complete patches, upgrades, and configuration changes as quickly as possible. However, this concept only goes so far. Without knowing and understanding the malicious activity unfolding, fast reactions only offer the illusion of defense; they are unlikely to thwart the aggressor's intent. The malicious activity will still ultimately be effective.

Conclusion

The Candidate Cyberspace Engagement Model addresses all of the differences between interactions in cyberspace and those in traditional physical domains enumerated in chapter 2 save one—speed of interactions. The six categories of cyberspace capabilities and their unintended flaws represent the first difference, namely that cyberspace is a created domain. Although the candidate model uses the physical infrastructure of a cyberspace, that infrastructure merely represents the entry fee that must be paid to interact in a cyberspace. The vast majority of interactions in the Candidate Cyberspace Engagement Model occur in the information domain, rather than the physical domain that the NCO CF has previously analyzed. This accounts for the second difference. Scenario two demonstrates the mechanics and effects of the third difference--stealth in cyberspace. The situational awareness capability attempts to expose stealthy capabilities in cyberspace. The candidate model also addresses the fifth difference, perishable advantage, by introducing a global schema that enumerates and tracks capability upgrades and versions as they are created and installed. Finally, the candidate model can represent the last difference—the different capabilities inside the whole of government, allied nations, and private entities. These different capability sets could account for the mixture of military, law enforcement, and private interests that may exist in a single cyberspace. However, the candidate model gives this diverse set of users a common schema to map their separate capabilities. Accounting for these differences gives the Candidate Cyberspace Engagement Model analytical utility beyond the traditional aspects of the NCO CF.

Chapter 4

Can the NCO CF Apply to Cyberspace Engagements?

If you are interested in democracy and its future,
you'd better understand computers.

Ted Nelson founder of Project Xanadu

In answering the central question of this thesis, whether the Network Centric Operations Conceptual Framework (NCO CF) can be applied to cyberspace engagements, Chapter 2 concluded that the NCO CF must at least be modified before it can be used to analyze cyberspace engagements. Insights from the NCO CF, the differences between cyberspace and traditional military operations, and the Candidate Cyberspace Engagement Model (Chapters 1, 2, and 3 respectively) produced a number of observations that added two important qualifiers to that conclusion and solidified the modifications to the NCO CF required if those qualifications are met.

Sharpness in a Virtual World

The characteristics of offensive and defensive interactions in cyberspace suggest that individual cyberspace engagements cannot be fought to a draw. An effective offense means an ineffective defense, and vice versa. So either the offensive action works or it doesn't. Either data is lost or it isn't. Either the offensive action is observed or it isn't. As a result, cyberspace engagements produce more absolute results when compared to traditional military operations.

The NCO CF measures effectiveness by the "degree to which strategic and PMESII (political, military, economic, social, infrastructure and information) objectives (are) were achieved."[1] The results of traditional military engagements can fall anywhere in a wide spectrum of

[1] John Garstka, "Network Centric Operations Conceptual Framework," ver 2.0 (draft), June 2004, 100.

effectiveness. For example, the Stryker brigade example previously discussed successfully met its objective, but still suffered a large number of combat losses. In contrast, cyberspace engagements only fall into three categories: mission accomplished and unobserved; mission accomplished and observed; or mission ineffective because of defensive measures. Therefore, the NCO CF's measures of effectiveness do not provide useful information in analyzing individual cyberspace engagements.

On an enterprise level, however, the command and control of individual cyberspaces and the interaction between separate cyberspaces (.com, .gov, .mil, NATO, CERT, etc.) begin to resemble the characteristics of the NCO CF. The challenge for defensive operations is to ensure that organic data is accurately shared while upgrades, patches, and configuration changes are applied across the federation of collaborating cyberspaces. Aggressors typically scan automatically for vulnerabilities. They can find and exploit vulnerabilities anywhere in the enterprise. The defense must be strong everywhere, while the offense only needs to be effective somewhere.

The NCO CF can be applied at the enterprise level over the course of numerous offensive cyberspace actions and defense responses. At this level, the performance of cyberspace defenders can be compared using the NCO CF to evaluate how and why one defense performs better than another. To perform such an analysis with the NCO CF, however, the offensive cyberspace campaign must be observable and consist of more than a single engagement. The NCO CF cannot analyze a cyberspace campaign that achieves its objectives in a single engagement since a baseline cannot be established.

The Critical Qualifier

The NCO CF can be useful in analyzing cyberspace campaigns, but only for those campaigns where the target cyberspace or its partners recognize that an attack is occurring or has occurred. Unlike stealthy

attacks in traditional military engagements that leave evidence of destruction in their wake, stealthy attacks or exploits in cyberspace may not leave any noticeable evidence of their presence, since information cannot be consumed. This creates a situation where cyber aggressors can bypass the entire NCO CF if they can keep the organic sensors in the target cyberspace from recognizing the attack or exploit actions.

This qualification is not only critical for employing the NCO CF, it is also critically important for real-world defensive operations. Cyberspace sensors and personnel must somehow obtain organic or shared information regarding the activities of offensive cyberspace actions. If not, offensive operations will have free reign inside the target's cyberspace.

Potential Updates to NCO CF

The elements of the NCO CF tied explicitly to the physical domain also apply to cyberspace operations even though cyber actions cannot be observed in the physical domain. While the draft of the NCO CF version 2 maintains that "Synchronization of Actions" and "Degree of Effectiveness" exist exclusively in the physical domain, synchronization and effectiveness are also critically important for cyberspace operations.[2] For example, if a patch used to prevent an attack is not consistently and correctly installed across a cyberspace (i.e. synchronized), then an aggressor can quite easily search out and find the gaps in the unsynchronized places. Likewise, if forces conducting traditional military operations require secure network services, one can measure the "Degree of Effectiveness" of cyberspace defenses even though they occur outside the physical domain. Since the concepts of "Degree of Actions Synchronized" and "Degree of Effectiveness" apply to cyberspace engagements occurring in the information (i.e. cyberspace) domain, then

[2] Reference Figure 6 in Chapter 1.

the NCO CF should be updated to apply these concepts to the information domain and not just the physical domain.

Half of this recommendation may have already been incorporated into the network enabled lexicon. Recent versions of the "Network-Enabled Command and Control Short Course" use an updated version of the Network-Enabled Value Chain seen in figure 14.

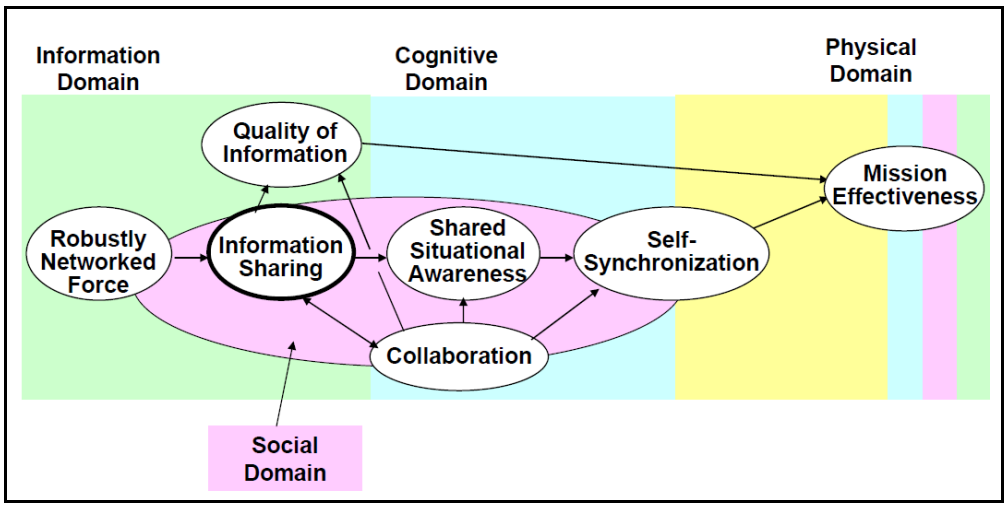


Figure 14: Updated Network Centric Operations Value Chain
(Reprinted from David Alberts, "Network-Enabled Command and Control Short Course," Module 2, Slide 21, http://www.dodccrp.org/files/nec2_short_course/NEC2%20Short%20Course%20Module%202%20-%20NEC2%20-%20%20Alberts%201-%2024%20-2010.pdf (accessed 8 Mar 2010))

Figure 14 shows "Mission Effectiveness" applied across all four domains. However, the information domain is still not included in the updated conceptualization of Degree of Decision Synchronization (i.e. Self-Synchronization in figure 14). Cyberspace defense operations, to be effective, must be synchronized across the defensive perimeter within the information domain. The Command and Control Research Program should update the Network Centric literature to apply the synchronization concept to the information domain so the NCO CF can provide more meaningful analysis with respect to cyberspace defense operations.

Addressing Speed of Interactions

The Candidate Cyberspace Engagement Model does not address the different speed of actions in cyberspace compared to traditional military operations (the fourth difference between traditional and cyberspace operations outlined in chapter 2). Humans decide when to launch offensive cyberspace operations. Once launched, these actions can hit with lightening speed. If such offensive capabilities are fully automated, attack or exploit actions can be completed before the human cyberspace defenders are even aware of what has happened, thereby making it impossible to mitigate the attack or exploit. In such a scenario, the defenders can only hope they have implemented effective automated responses.

Cyber defenders can automate responses in three ways. The first is to use tools that automatically find vulnerabilities before an attack. Existing tools, such as the Security Content Automation Protocol, help automate vulnerability management, measurement, and policy compliance evaluation.[3] Once identified, these vulnerabilities can be mitigated before an attack occurs. Successful use of these tools requires both good configuration control and remediation capabilities. Next, response actions can be pre-coordinated and built into the defensive perimeter to respond during an attack. This method depends upon the cyberspace defense community building a shared awareness that is correct and synchronized. Finally, defenders can automate their responses by employing tools sophisticated enough to sense an attack occurring inside the defensive perimeter and stop it before it is effective.

Configuration control is a key prerequisite for automating Computer Network Defense. According to one JTF-GNO Liaison Officer, the Department of Defense, unfortunately, has just begun to take steps

[3] National Institute of Standards and Technology, "The Security Content Automation Protocol," scap.nist.gov (accessed 29 May 2010).

towards comprehensive configuration control of its computer networks.[4] Without it, cyberspace defenders cannot confidently know what capabilities are deployed, where they are deployed, how they are deployed, and subsequently control how they are configured. Because of the lack of configuration control, mitigation of the numerous attacks on DoD systems requires significant human intervention.

Maintaining configuration control can be just as challenging on classified networks. Following the 2008-2009 Conflicker attacks, "it took 45 days for STRATCOM to get a count of the number of SIPRNET machines on DOD networks."[5] While defenders try to devise methods to prevent attacks from occurring in the future, aggressors might capture the targeted information and install a backdoor that allows similarly dangerous, but stealthy and fully automatic, actions in the future.

Figure 12 can be used to illustrate the difference between an automated and manual defense process. It shows the defensive recognition of an intrusion occurring at step five. Defenses could be improved by automatically identifying the attack after step one and automatically responding to prevent further intrusion (step 3) and exploitation (step 4). Depending on the tools, skills, and target, the time required for the aggressors to move through steps two through four could take less than a second or as long as a few weeks. Ideally, defenses would protect the cyberspace from attack or exploitation in the first place. The next best defensive response would be to thwart the attack as it unfolds. Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and the situational awareness tools discussed in chapter 2 can help to accomplish this task. Non-automated defenses must recognize the situation and respond quickly enough to prevent

---

[4] Danette Wile (Joint Task Force-Network Operations liaison to 24th Air Force), in discussion with the author, 19 Feb 2010.

[5] General Kevin Chilton, in a speech to the United States Air War College, 10 March 2010. He followed up this point by remarking that he wasn't confident that the final number presented was accurate.

exploitation from occurring. Such defenses cannot do so when offensive actions occur in seconds.

The NCO CF can evaluate cyberspace defense operations whether the response tools are automated or controlled by humans. However, the automated tools should be considered a parallel synthetic instantiation of the NCO CF. This parallel processing of defense actions uses artificial intelligence or heuristics to virtualize the cognitive and social domains. In this way, the automated tools mimic the NCO CF concepts of individual and shared sense making, collaborate with similar automated defenses, make quality decisions, and synchronize actions automatically. The NCO CF can effectively evaluate the automated cyber defense processes restricted to the information domain since they involve processes similar to those spanning the cognitive, social, and physical domains and there would be data to evaluate. However, while these automated processes are occurring, human cyberspace defenders are augmenting the automated defenses by looking for attacks and exploits the automated defenses miss, areas the machines cannot defend, or repairing services that are malfunctioning. Any evaluation of cyberspace using the NCO CF must consider both the automated and human-driven processes separately, since they simultaneously address different problems, and holistically, since they complement each other. These parallel processes would recombine in the Degree of Mission Effectiveness concept to measure how well they work together to achieve the cyberspace defense mission.

Beyond the Department of Defense

In the United States, only the national military and intelligence forces can legally attack and exploit the cyberspaces of foreign entities. Therefore, the cyberspace response activities of the Department of Homeland Security (DHS) and private industry are purely defensive in nature. Accordingly, these entities are not empowered to use attack or exploit cyberspace capabilities. As a result, private industry and DHS

must collaborate with the DoD if they want to counter-attack or exploit an aggressive act underway. Figure 15 below shows a representative example of the external parties that any organization may need to work with during a computer security incident.

Figure 15 – Collaboration With External Organizations
(Reprinted from National Institute of Standards and Technology, "NIST Computer Security Incident Handling Guide (Special Publication 800-61 Revision 1)", (Gaithersburg, MD: 2008), 2-5)

Collaborating outside one's cyberspace benefits all cyberspace-defending organizations since it involves sharing organic information across an extended network. As seen in the NCO CF case studies, sharing information can dramatically improve the "Degree of Shared Information" and "Quality of Shared Information" since collaborating networks share more data, observations, knowledge and sensors.

Defenders of completely separate cyberspaces can also collaborate. In effect, these separate defenders can take advantage of the separation between different and non-cooperating aggressors to improve their collective defenses. A natural separation develops between aggressors who want to maintain anonymity and secrecy, while most defenders will be willing to work together to improve their individual defenses. In such an environment, once one of the cooperating cyberspace defenders

identifies a vulnerability or exploit, collaboration among the rest helps update the defenses of all separate, but cooperating, cyberspaces.[6]

Formalized and well-coordinated collaboration can help the collective whole establish firmer control of even large cyberspaces like the Internet. For example, if an aggressor launches a Distributed Denial of Service (DDoS) attack, collaborating entities could dramatically limit its effectiveness. Once a DDoS attack is recognized as such, each collaborator would block malicious DDoS traffic and inform upstream providers and other collaborators to do the same.[7] This example highlights how defenders controlling pieces of the Internet can work together to defeat the actions of a malicious network. If the relative number of participants is large enough, the attack could be stopped completely, have a significantly reduced impact on the cyberspace target, or severely impact those who are not defensive collaborators.

The NCO CF does not specifically limit itself to collaboration within military channels. The framework, however, does not evaluate the diversity or quality of collaborators even though its quality of interactions concept includes quantity, reach, and richness attributes. As seen in figure 15 and the DDoS example above, cyberspace defenders can benefit both from a wide variety and a large number of helpful collaborators. To be useful in cyberspace analyses, the NCO CF's quality of interactions concept should include an attribute evaluating the diversity of organizations and the quality (i.e. helpfulness) of collaborators.

---

[6] Obviously this logic does not hold up if the knowledge of the vulnerabilities spreads to the aggressors as well. Release of the vulnerabilities into the public domain is a part of this risk.

[7] Mirkovic, Jelena, Max Robinson, Peter Reiher and George Oikonomou, "Distributed Defense Against DDoS Attacks," University of Delaware Technology Report, 6 Jul 2004, http://www.cis.udel.edu/~sunshine/publications/udel_tech_report_2005-02.pdf (accessed 30 Mar 2010) and Katerina Argraki and David Cheriton, "Scalable Network-layer Defense Against Internet Bandwidth-Flooding Attacks," IEEE/ACM Transactions on Networking, vol. 17, num. 4, 2009, 1284-1297, http://infoscience.epfl.ch/record/128395 (accessed 30 Mar 2010).

Conclusion

Although the NCO CF was originally developed to model traditional military operations, the analysis above shows that it can, with some qualifications and modifications, evaluate one of its components, namely the "Network Enabled Force." The analysis also suggests complexities hidden in network capabilities for which the NCO CF does not account. More to the point, the NCO CF assumes the perfect delivery of cyberspace capabilities without considering cyberspace vulnerabilities. The Candidate Cyberspace Engagement Model reveals that the duality of offensive actions in cyberspace can negate this assumption.

As a result, the NCO CF must meet a couple of qualifications and be updated before it can be usefully applied to cyberspace engagements. If the qualifications of multiple engagements and observable offensive actions are not met, the NCO CF cannot be usefully employed. Furthermore, unless the NCO CF is updated to apply the synchronization concept to the information domain, include the parallel evaluation of automated and human-driven defense tools, and add attributes for the diversity and quality of collaborators, it will miss some of the significant differences between cyberspace engagements and traditional military operations.

Conclusion

We can't solve problems by using the same kind of thinking we used when we created them.

Albert Einstein

The rise in the significance of the infosphere, the fifth dimension of strategy, cannot be ignored. Like the other dimensions, strategy in the infosphere has its own character, and requires operations, organizations and career paths that are specific to its unique nature.

David Lonsdale in The Nature of War in the Information Age

While the nature of war rings eternal, the use of information in war over the last few decades has dramatically increased and changed how future wars can be conducted. From satellite links, to remotely piloted aircraft, to the distributed common ground system, to a platoon in a firefight, the desire for information in war is insatiable. Cyberspace's raison d'être, as shown by Metcalfe's law, comes from connecting more entities together to share an ever-increasing amount of operational information.[1] As evidenced by the recent stand-up of the United States Cyber Command, the DoD continues to take steps to organize its forces and write its doctrine to take advantage of the capabilities inherent in cyberspace networks.

The Network Enabled Value Chain (original version shown in figure 4 and updated version shown in figure 14) attempted to explain why information capabilities can make significant differences in war. The

[1] Robert Metcalfe postulated that the value of a telecommunications network is proportional to the square of the number of connected users. Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law is Wrong," IEEE Spectrum, July 2006, http://spectrum.ieee.org/computing/networks/metcalfes-law-is-wrong (accessed 29 May 2010). Others disagree on the specific equation, but all agree it increases in a non-linear manner.

authors of the Network Centric Operations Conceptual Framework (NCO CF) built it upon the logic of the value chain to explain how cyberspace can make a difference in combat and provide analytic measures to compare the effectiveness of military operations. The networks that improved the effectiveness of military operations soon became a highly contested domain of war in their own right. However, since cyberspace is not tangible like the other warfighting domains, conflicts in cyberspace differ significantly from traditional military conflicts.

Acknowledging the primary differences between cyberspace engagements and traditional military operations, the Candidate Cyberspace Engagement Model provides a framework for understanding and tracking offensive and defensive actions during cyberspace exploitations and attacks, and identifying their root causes. Insights from the Candidate Cyberspace Engagement Model lead to some important qualifications and updates that must be applied before analysts can use the NCO CF to evaluate cyberspace conflicts.

The process of analyzing the NCO CF with respect to cyberspace, examining the differences between cyberspace engagements and traditional military engagements, and developing the Candidate Cyberspace Engagement Model raised a number of additional insights regarding cyberspace. These insights, outlined below, revolve around the duality of a cyberspace engagement (i.e. the offense and defense), the flaws and vulnerabilities that make cyberspace engagements possible, and the ends for which they fight. The final section of the conclusion returns to the Candidate Cyberspace Engagement Model to suggest some enhancements that could improve its utility in analyzing cyberspaces.

Keys for Offensive Actions in Cyberspace

Personnel controlling offensive actions must recognize the perishablility of any advantage they hold and carefully consider the right time and place to use their tools. On the one hand, offensive tools are more likely to be successful if first used against larger cyberspace

targets, since their increased complexity and traffic will better mask the attack. Likewise, an attack against a bigger cyberspace could yield more intelligence. On the other hand, larger cyberspaces will generally employ more sophisticated and more numerous cyberspace defenses. These defenses increase the likelihood of not only thwarting, but also identifying the offensive action. Therefore, attacks against bigger cyberspaces are more likely to be detected. The repeated use of attack tools also increases the likelihood of getting caught. Once detected, the chance of successfully employing the tool again is dramatically decreased while the likelihood of the target turning the tables to exploit the offensive action increases. Therefore, cyberspace strategists should continue to regard military attack systems and methods as strategic national secrets: Carefully protected and cautiously used.

The synthesis of insights from the Candidate Cyberspace Engagement Model and NCO CF indicates two additional considerations important to offensive actions. First, offensive operations rely upon a strong awareness of an adversary's cyberspace. If an aggressor already knows that an automated offensive action will successfully capture targeted information and the target cannot respond in time to prevent exfiltration, the aggressor has a decidedly upper hand. Second, if aggressors must choose between tools that are automatic and tools that are stealthy, they should choose stealthy ones in almost all situations. Undetected attacks are unlikely to tip off targets to the presence of a vulnerability, therefore such attacks will likely remain available for future use, unless the defenders patch it by chance.

Keys for Defensive Actions in Cyberspace

In an ideal world, cyberspace defense would only need to focus on the inherent vulnerabilities of a cyberspace. Unfortunately this would require the elimination of all flaws in cyberspace capabilities. While the development community must try seriously to create flawless software, it is unrealistic to assume that developers can achieve this ideal given the

history of cyberspace capabilities. Provided that cyberspaces will continue to be flawed, defensive operations must quickly instigate stop-gap measures when any vulnerability is identified and then rapidly and comprehensively install fixes when available. Cyberspace defenders should continue to press for more and better automated tools to ensure the quickest possible response.[2]

The best cyberspace defense is self-aware, self-synchronized, and responds to emerging threats at machine speeds. Artificial intelligence and automated tools can help improve defense capabilities, but humans still have to discover what the automated tools have missed and adjust defenses accordingly. Cyberspace defenders could consistently improve the automated defense posture of their cyberspace by adopting a "Tune up, and Tune Out" mentality. Defenders would always focus on searching, upgrading, and improving the automated defense tools (i.e. tune up) that improve the ability of the system to automatically tune out attacks at machine speed.

Speed, standardization, and collaboration are important when relying upon human feedback to improve defenses. Speed is imperative since some attacks and exploits take time to complete and can be mitigated through fast defensive reaction. Standardized cyberspace configurations increase the defense's understanding and simplify control. According to John Gilligan, former Air Force Chief Information Officer, "80 percent of breaches were tied to software configuration irregularities."[3] Since vulnerable cyberspaces are logically dispersed and can be struck at any time, defenders must collaborate with allies and partners to realize synergies involved in sharing observations and better

---

[2] Automated defenses must be tuned appropriately to continue providing capability to the user, even though there is suspicious activity occurring. Tools such as IDS and IPS tend to block authorized traffic much more frequently than desired.

[3] Wyatt Kash, "Software Configuration Controls Essential to Cybersecurity,"", Government Computer News, 17 Feb 2010, http://gcn.com/Articles/2010/02/17/Software-configuration-controls-essential-to-cyber-security.aspx, (accessed 18 Feb 2010).

protect the vulnerable cyberspaces. Unlike the military centric collaboration implied in the NCO CF, cyberspace defense collaboration should extend well beyond typically military channels. This type of collaboration should emphasize the importance of organic information, shared through effective collaboration to enhance global situational awareness.

The Cost of Creating Vulnerabilities

The flaws in cyberspace capabilities are the genesis of cyberspace engagements. A cyberspace capability enables or inhibits attack capabilities depending on the physical characteristics and unintended vulnerabilities of the cyberspace utility. If there were no flaws, remote exploitation would not be possible and attacks could only follow the physical properties of the cyberspace environment.[4] The physical characteristics are more likely inherent vulnerabilities (discussed in Chapter 3) that cannot be changed, but must be recognized, limited, and monitored as necessary. If attacks were limited to those that target inherent vulnerabilities, the costs of defending a cyberspace would be considerably reduced.

There are a few practical ways to reduce the unintentional flaws as well as mitigate the inherent vulnerabilities in the cyberspaces used within the DoD. First, the department could dramatically improve its ability to provide enterprise-wide configuration control. In conjunction with this first step, the DoD should track the vulnerabilities of the software that it uses in its cyberspaces. This inventory could utilize and contribute to the work that has already been completed with the Common Vulnerability and Exposures (CVE) dictionary.[5] Next, the department could determine where, how much, and what type of defense

---

[4] Implied in this statement is the fact that insiders could still cause damage, but not because of design flaws.

[5] MITRE, "MITRE Celebrates a Decade of Software Security with CVE," 21 Oct 2009, http://www.mitre.org/news/releases/09/cve_10_21_2009.html, (accessed 1 April 2010).

should be deployed using a holistic objective analysis of its cyberspaces. This analysis could incorporate many of the CCEM enhancements suggested below to determine the top priorities in cyberspace defense. Finally, the department could motivate cyberspace developers to become security conscious by objectively assessing the security of cyberspace capabilities they have developed in the past, and use such assessments as a criteria in awarding future cyberspace development contracts. In conjunction with this step, developers should be evaluated on how quickly and completely they fix identified vulnerabilities.

Benjamin Franklin once said that "an ounce of prevention equals a pound of cure." Given the costs of curing and risks of not curing vulnerabilities in military cyberspace, the DoD would be wise to improve vulnerability prevention by proactively pursuing more secure software. Considering the benefits, importance, and complexity of creating secure cyberspace capabilities, the DoD should build an umbrella concept of "Cyberspace Creation Operations" on par with offensive and defensive operations. There are currently a few scattered efforts, such as the softwareforge open source software initiative and the DoD enterprise architecture, which would fall under this umbrella.[6] While there are a number of cyberspace development programs in the DoD, the policies guiding them are disjointed and development efforts are not synchronized holistically. Formalizing "Cyberspace Creation Operations" would give this area the focus, organization, and career pathways required to develop expertise and procure consistently more secure cyberspace capabilities.

---

[6] The Defense Information Systems Agency's Softwareforge concept is explained here http://disa.mil/forge/ (accessed 5 May 2010) and Tim Bass and Roy Mabry, "Enterprise Architecture Reference Models:
A Shared Vision for Service-Oriented Architectures," (draft version 0.81 for submission to IEEE MILCOM 2004), 17 Mar 2004, 1, http://www.enterprise-architecture.info/Images/Defence%20C4ISR/enterprise_architecture_reference_models_v0_8.pdf, (accessed 5 May 2010).

Risks can outweigh the utility

War fighters who use cyberpower to maximize mission effectiveness must be cognizant that cyberspace capabilities also create potential vulnerabilities. As with any tool, the more integral it is to operations, the greater the impact when it is disrupted or taken away. As Gen Mattis, Commander of United States Joint Forces Command said, "a well-timed and executed cyber attack may prove just as severe and destructive as a conventional attack."[7]

The more important the connections, controls, or information present in a cyberspace, the more dangerous the vulnerabilities become. In fact, some scenarios show that the damage of a successful attack may be much greater than the utility the original cyber tool provided. As an extreme example of this point, consider an electrical company connecting its control system for the electrical grid to the Internet without any security. In such a scenario, shutting down that grid would be a trivial matter. So while the company connected the controls to the Internet in order to increase ease of control and decrease costs, the vulnerability of those controls would also allow remote access by anyone with the knowledge or tools to take advantage of those vulnerabilities. The electrical company did not intend to let unknown individuals control or shut down the grid, but establishing such connections created unintended vulnerabilities disproportionately larger than the benefit they provided.

Cyberspace must be defended in order to protect its utility. Otherwise, cyberpower may end up like the hair that gave strength to the biblical character Samson. Once it was cut, he was weakened and his enemies successfully attacked.[8] The more important the capability, the

---

[7] General James Mattis, statement before the House Armed Services Committee, 18 Mar 2009, http://smallwarsjournal.com/blog/2009/03/general-james-mattis-before-th/.
[8] Judges, chap 14-16, (New International Version) http://www.biblegateway.com/passage/?search=Judges%2014-16&version=NIV. It

more seriously the operators should consider its security and question the necessity of any cyberspace connections.

Potential Expansion of the Candidate Cyberspace Engagement Model

As previously described, the Candidate Cyberspace Engagement Model can help analysts understand the risks for each node in a cyberspace. An updated model could extend this framework to make a numerical or comparative assessment of nodal risk based on the current inventory of cyberspace capabilities cross referenced against the CVE table. The model could be further extended to evaluate the vulnerabilities of an entire cyberspace by aggregating the risks of all the capabilities currently operating at each node. Since the result would be a summation of individual nodes, the analysis could also provide specific details that analysts can use to conduct what-if analyses. These analyses would show why some cyberspaces are more vulnerable than others and point to ways of reducing vulnerabilities while maintaining capabilities. Additional factors that analysts could use include: historical security performance of cyberspace capabilities, degree of cyberspace situational awareness, degree of cyberspace control, number of cyberspace gateways, and degree of defense in depth (number, variety and performance of defense capabilities). Analysts taking account of all of these factors could not only provide a richer understanding of defensive actions, but could also recommend future capability improvements.

Conclusion

Since the United States is systematically using cyberspace throughout its military, government, economic, and social domains, it has more potential cyberspace vulnerabilities than a country with limited electrical and cyberspace implementations. Likewise, a potential enemy's use of cyberspace capabilities will determine their potential cyber

---

should also be noted that Samson's hair eventually grew back and he killed his enemies.

vulnerabilities. However a country or non-state actor's ability to attack depends more on their technical knowledge of offensive tools than on their extensive use of cyberspace. This is why individual actors, terrorist groups or relatively underdeveloped states threaten the United States' interests through cyberspace. The United States' intense use of cyberspace utilities necessitates that the country protects them well.

Cyberspace vulnerabilities are being attacked and exploited every day. China's People's Liberation Army proposed the idea of unrestricted warfare using non-military methods of war in future conflicts which will "have the same or more destructive force than military warfare."[9] Many of these methods, such as media warfare, network warfare, technological warfare, and fabrication warfare use cyberspace to pursue their political objectives.[10] Closer to home, US power grids, telecommunications trunks, and air traffic control systems have already been attacked successfully through cyberspace.[11] Many computer security experts in the United States believe the country remains vulnerable to this kind of cyber attack and warn of a large, coordinated attack that could disrupt power, telephone, banking, media and fuel nationwide for months, thereby quickly bringing the United States to its knees.[12] If indeed possible and successful, such an attack would demonstrate cyberpower independently achieving policy objectives, albeit in a non-military way, according to the Chinese labels.

---

[9] Qiao Liang and Xiansui Wang, *Unrestricted Warfare*, (Beijing: PLA Literature and Arts Publishing House, 1999), 117, http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf.
[10] Liang and Wang, *Unrestricted Warfare*, 55.
[11] O. Sami Saydjari et al. "Letter to President Bush," 27 Feb 2002, http://www.uspcd.org/letter.html (accessed 8 March 2010).
[12] O. Sami Saydjari, "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action," testimony before the House Committee on Homeland Security, subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 25 April 2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf (accessed 8 March 2010).

The Chinese unrestricted warfare doctrine seeks to turn a US strength into a weakness and it stands as a warning to the United States' military and national leaders. The economic and military strength that the United States is deriving from cyberpower is also increasing its vulnerability both inside and outside the military sphere. To lay it bare, because the United States draws its power from an information-based economy which relies on vulnerable cyberspace Internet connections, cyberspace has opened a strategic vulnerability. Chinese unrestricted warfare doctrine targets this vulnerability, but the DoD does not protect non-military cyberspaces. Who is going to protect the United States' "peace and security" in this regard? The administration must address some difficult questions regarding jurisdictions lest these non-military vulnerabilities remain open. Susan Brenner has suggested that a Cyber Security Agency which blends law enforcement and military authorities together provides a useful starting point.[13] Such an agency could coordinate cyberspace defense findings with the programmers who created the physical and syntactic tools, companies who provide security products, and US cyber-attack forces. By filling a dual law-enforcement and military role, this agency could also coordinate criminal cases, request diplomatic action, and coordinate military action. This new type of agency would help the United States respond to state and non-state actors conducting crime, terrorism, or war through cyberspace.

Cyberspace as a domain in its own right, as opposed to an adjunct enhancement to the other domains, is still a relatively young concept. The NCO CF serves as a useful starting point to analyze offensive and defensive activities in cyberspace. The development and integration of cyberspace capabilities is a process, not a destination. The message of the DoD's 2001 Report to Congress is still true:

---

[13] Susan Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*, (New York, NY: Oxford University Press, 2009), 296.

> Network Centric Warfare should not be misconstrued as a fully developed and deployable warfighting capability. It is not. Far more needs to be done to transform today's platform-centric force into a network-centric one. Far more needs to be done to develop, test, and refine network centric concepts of operation and co-evolve them with doctrine, organization, command approach, systems, and the other components of a mission capability package. Considerable effort will also be required to develop network-centric capabilities that can effectively be employed in Allied and coalition operations.[14]

The NCO CF and Candidate Cyberspace Engagement Model are imperfect tools, but they begin to uncover and analyze some of the hidden terrain of cyberspace. Analysts can use and expand on these tools to further illuminate cyberspace activities and inform the options provided to the decision makers.

The insights above can help strengthen the military's understanding of the domain and focus the development of cyberspace research into the most critical areas. Top priority research and procurement items should include: creating secure capabilities, improving cyberspace situational awareness, automating defenses, and developing stealthy attacks and exploits. In the end, cyberpower has not changed Clausewitz's nature of war, but cyberpower could change the character of war with a single keystroke. A keystroke is quite a low threshold to cross.

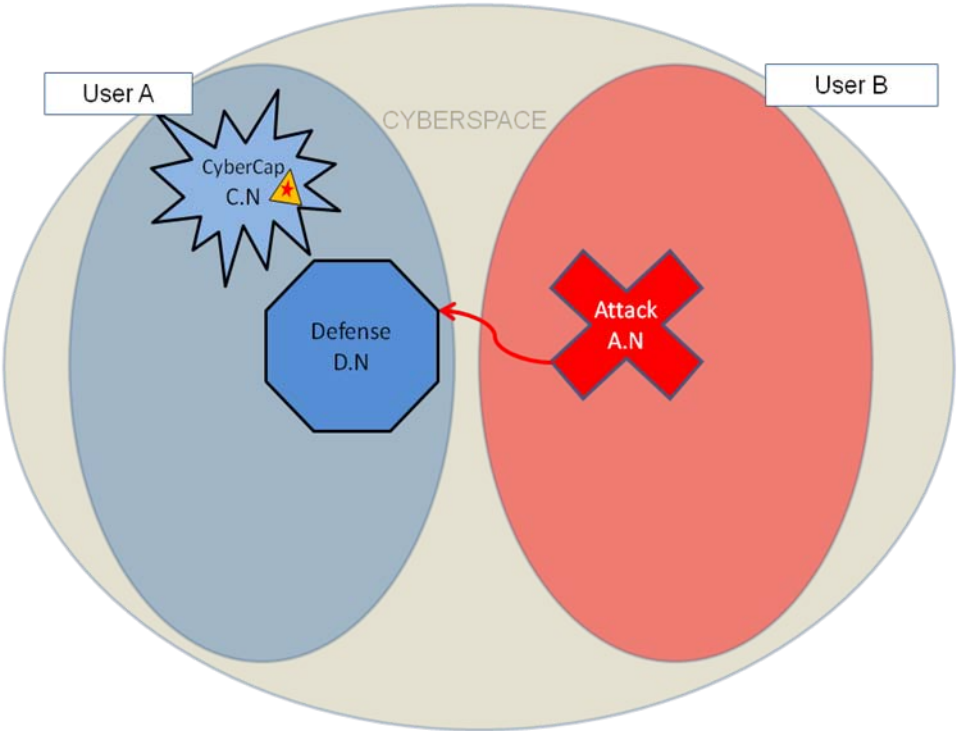
---

[14] Department of Defense, *Network Centric Warfare Report to Congress*, July 2001, i, http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf (accessed 8 Mar 10).

Appendix A – Basic Cyberspace Engagement Scenarios

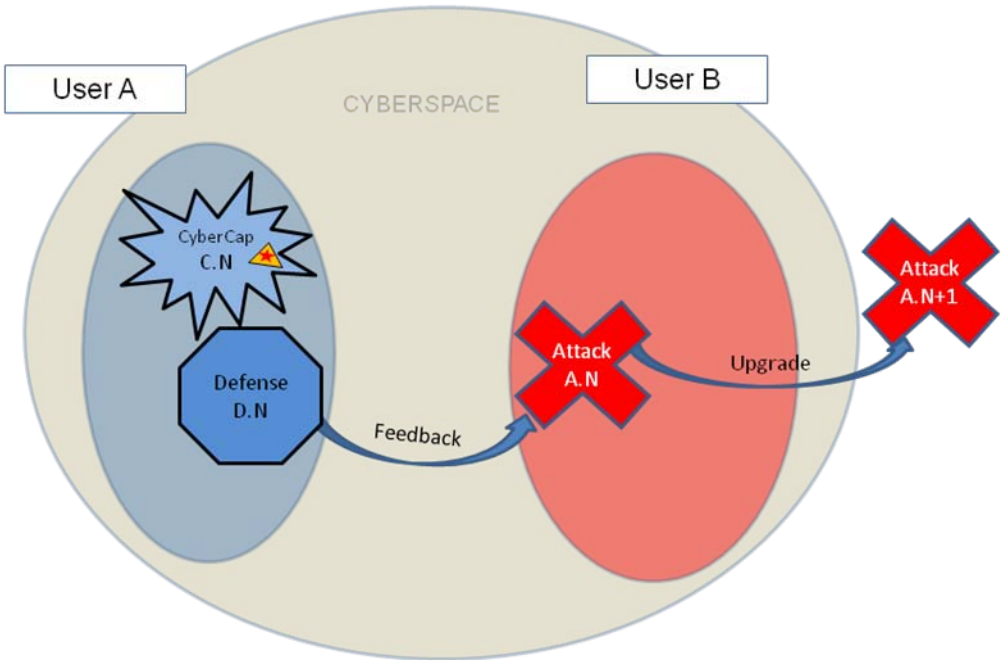
Basic Cyberspace Engagement Scenario 1: Defense Stops Attack or Exploitation

Step 1 – User B launches attack capability A.N against User A



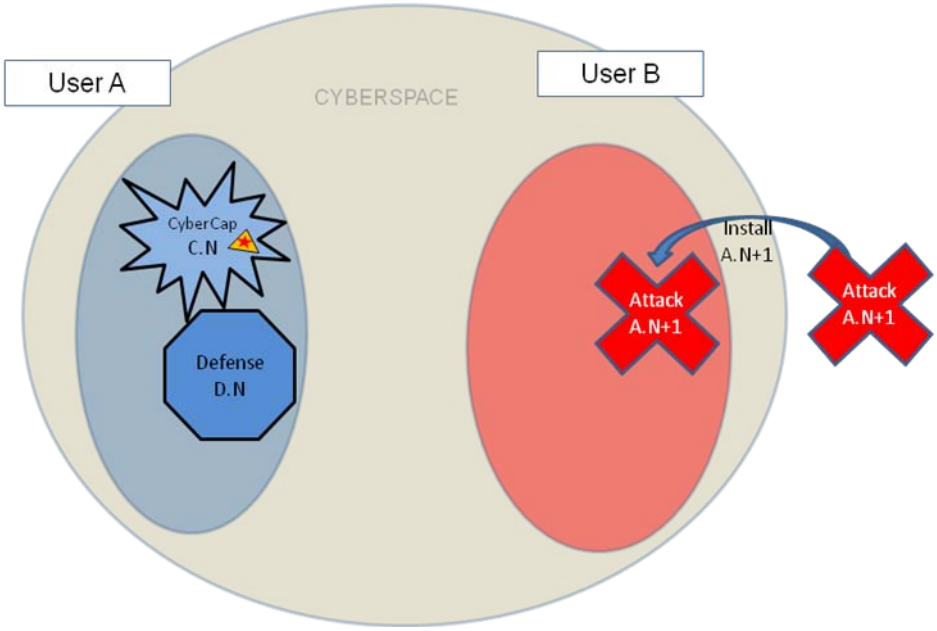
Result – Defense capability D.N thwarts Attack A.N, thus preventing User B from accessing User A's portion of the shared cyberspace

Step 2 – User B observes that Attack A. N did not work.



Result – User B upgrades attack capability A.N to attack capability version A.N+1 (or creates a new attack capability A+1.0).

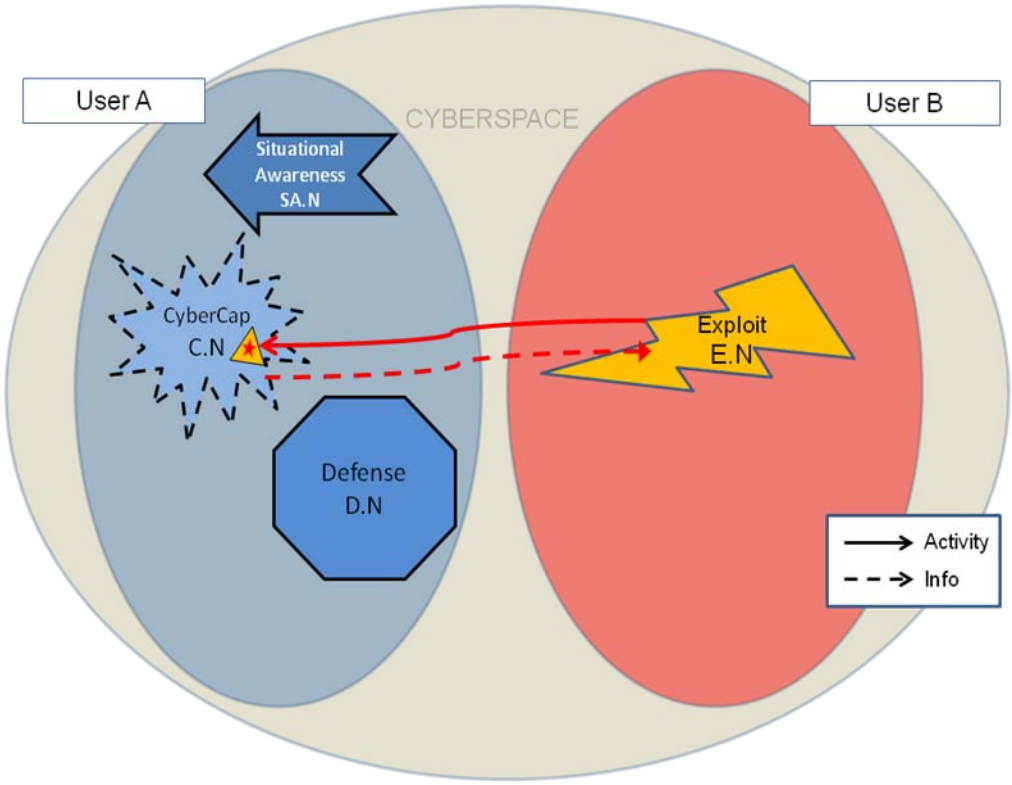
Step 3 – User B completes upgrade of A.N+1 installs A.N+1



Result – User B returns to step 1 to launch another attack which may go into any of the three scenarios described herein.

Basic Cyberspace Engagement Scenario 2: Ineffective Situational Awareness and Defense

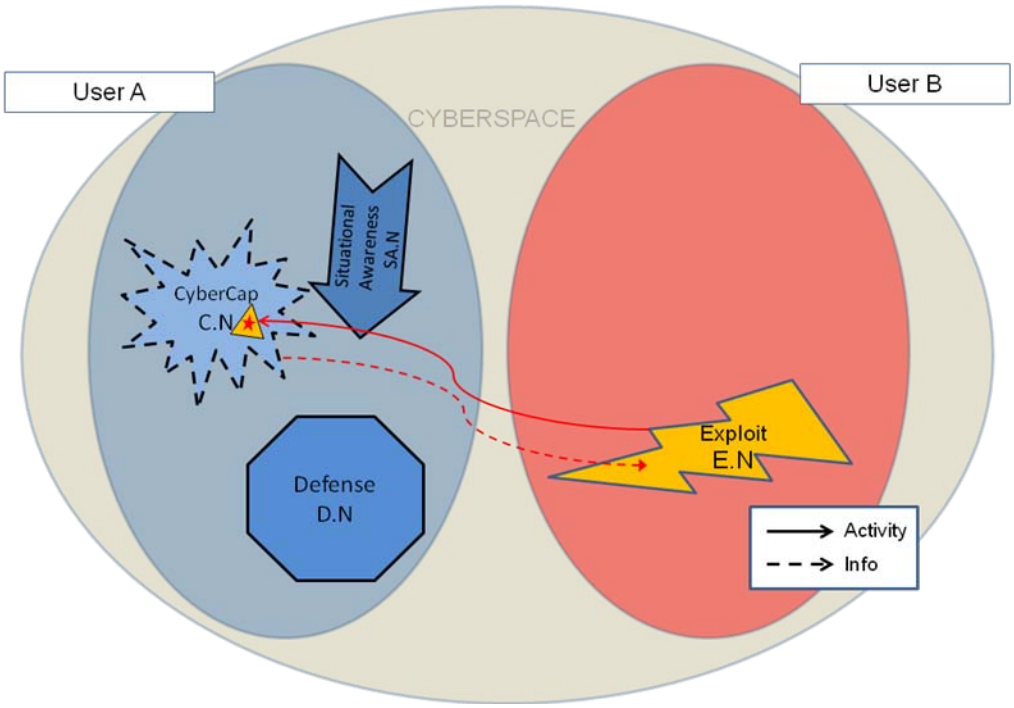
Step 1 – User B successfully launches an undetected exploit E.N against User A. SA.N and D.N are ineffective and C.N is exploited (as denoted by the dashed borders).



Result – User C can collect, disrupt, deny, degrade, or destroy User A's information. Since the exploit went undetected, User B can repeat E.N as desired.

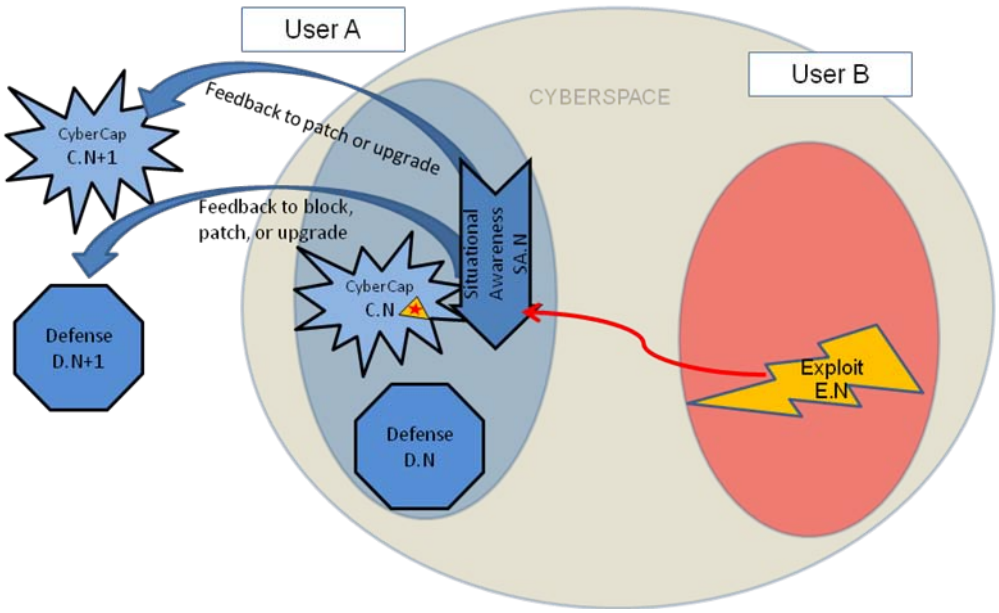
Basic Cyberspace Engagement Scenario 3: Ineffective Defense, Effective Situational Awareness and Defense

Step 1 – User B successfully launches exploit E.N against User A, but is detected by user A's situational awareness capability SA.N.



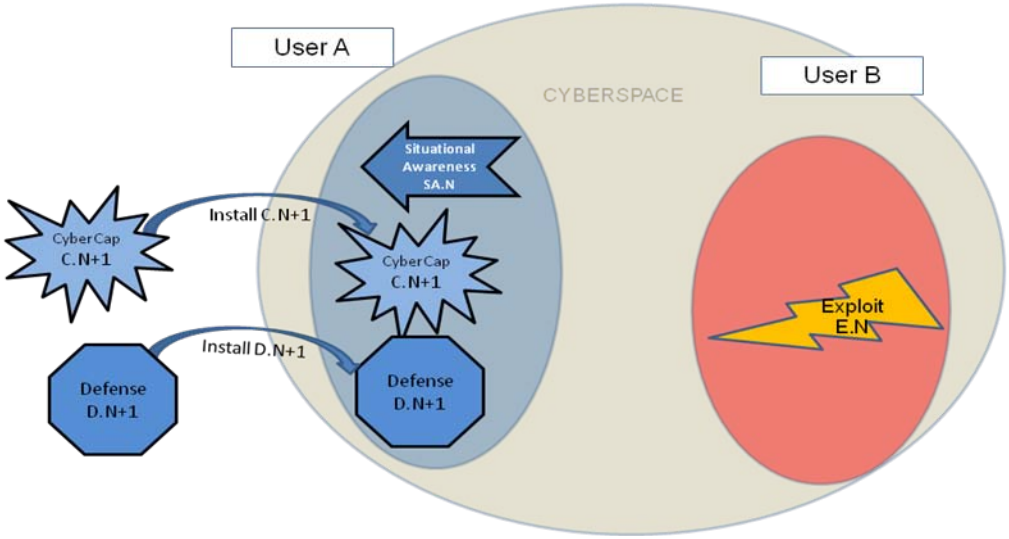
Result – User B can collect, disrupt, deny, degrade, or destroy User A's cyberspace capability C.N for a limited time.

Step 2 – User A provides feedback to creators of C.N and D.N.



Result – Creators and operators of C.N and D.N make adjustments and develop upgrades to prevent exploit E.N from being successful the next time it is launched against User A's cyberspace.

Step 3 – User A installs C.N+1 and D.N+1. (Note these installations will likely not occur at the same time)



Result – Exploit E.N is no longer effective against User A's cyberspace. This returns both parties to scenario 1.

BIBLIOGRAPHY

Academic Papers

Kaplan, Jeremy. "A New Conceptual Framework for Net-Centric, Enterprise-Wide, Systems-of-Systems Engineering." Working Paper, Center for Technology and National Security Policy, National Defense University, June 2006. http://www.ndu.edu/CTNSP/docUploaded/DTP%2030%20A%20New%20Conceptual%20Framework.pdf (accessed 8 Mar 2010).

Mirkovic, Jelena, Max Robinson, Peter Reiher and George Oikonomou, "Distributed Defense Against DDoS Attacks," University of Delaware Technology Report, 6 Jul 2004. http://www.cis.udel.edu/~sunshine/publications/udel_tech_report_2005-02.pdf (accessed 8 Mar 2010).

Articles

Argyraki, Katerina and David R.Cheriton. "Scalable Network-layer Defense Against Internet Bandwidth-Flooding Attacks." IEEE/ACM Transactions on Networking, Volume 17, Number 4, 2009. http://infoscience.epfl.ch/record/128395 (accessed 8 Mar 2010).

Barlow, John Perry. "The Next Economy of Ideas: Will copyright survive the Napster Bomb? Nope, but creativity will." *Wired*, October 2000. http://www.wired.com/wired/archive/8.10/download_pr.html (accessed 7 May 2010).

Bass, Tim and Roy Mabry. "Enterprise Architecture Reference Models: A Shared Vision for Service-Oriented Architectures." Draft version 0.81 for submission to IEEE MILCOM 2004, 17 Mar 2004. http://www.enterprise-architecture.info/Images/Defence%20C4ISR/enterprise_architecture_reference_models_v0_8.pdf (accessed 5 May 2010).

Cebrowski, VADM Arthur K., USN and John J. Garstka, "Network Centric Warfare: Its Origin and Future." *Proceedings of the Naval Institute,* Volume 124, Number 1, January 1998. http://www.kinection.com/ncoic/ncw_origin_future.pdf (accessed 8 March 2010).

CERT Coordination Center. "Denial of Service Attacks." 4 June 2001. http://www.cert.org/tech_tips/denial_of_service.html (accessed 30 May 2010).

Cisco Systems Inc. "Internetworking Basics." http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html (accesed 27 May 2010).

Colecchia, Alessandra and Paul Schreyer. "ICT Investment and Economic Growth in the 1990s: Is the United States a Unique Case? A Comparative Study of Nine OECD Countries." *Review of Economic Dynamics*, Volume 5, Issue 2, April 2002. http://www.tos.camcom.it/Portals/_UTC/Scenari/I001.pdf (accessed 9 May 2010).

Coleman, Kevin. "Cyber Situational Awareness." *Defensetech*. http://defensetech.org/2010/01/18/cyber-situational-awareness/ (accessed 29 March 2010).

Fulghum, David. "Cyber-Warriors Begin Training." *Aviation Week*, 29 Mar 2010. http://www.aviationweek.com/aw/jsp_includes/articlePrint.jsp?storyID=news/awst_032910_p48.xml&headLine=null (accessed 31 March 2010).

Harris, Shane. "The Cyberwar Plan," *National Journal Magazine*, 14 Nov 2009. http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed 14 Dec 09).

"Homeland Security Seeks Cyber Counterattack System." *CNN.com/technology*, 4 Oct 2008. http://www.cnn.com/2008/TECH/10/04/chertoff.cyber.security/ (accessed 24 Mar 2010).

Johansson, Jesper. "Security Management – The Fundamental Tradeoffs," *Microsoft: Technet*. http://technet.microsoft.com/en-us/library/cc751266.aspx (accessed 7 May 2010).

Kash, Wyatt. "Software Configuration Controls Essential to Cybersecurity." Government Computer News, 17 Feb 2010. http://gcn.com/Articles/2010/02/17/Software-configuration-controls-essential-to-cyber-security.aspx (accessed 18 Feb 2010).

Liles, Sam. "Into the Darkness of Cyberspace." *Selil.com*, posted on 9 Mar 2009. http://selil.com/?p=645 (accessed 15 Dec 09).

O'Reilly, Tim. "Open Source Paradigm Shift." Jun 2004. http://tim.oreilly.com/articles/paradigmshift_0504.html (accessed 30 Nov 2009).

Office of the Assistant Secretary of Defense for Networks and Information Integration. "DoD Information Assurance Strategic Plan." August 2009, 1, http://cio-nii.defense.gov/docs/DoD_IA_Strategic_Plan.pdf.SANS Institute. "Top Cyber Security Risks." Sep 2009. http://www.sans.org/top-cyber-security-risks/ (accessed 29 Mar 2010).

Books

Alberts, David, et al. *Understanding Information Age Warfare*. Washington, DC: Command and Control Research Program, 2001.

Alberts, David and Richard Hayes. *Power to the Edge: Command and Control in the Information Age*. Washington, DC: Command and Control Research Program, 2003.
Arquilla, John and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information* Age. Santa Monica, CA: RAND, 1997.
Axelrod, Robert. *The Evolution of Cooperation*. Cambridge, MA: Persues Book Group, 2006.
Bell, Daniel. *The Cultural Contradictions of* Capitalism. New York, NY: Basic Books, 1996.
Brate, Adam. *Technomanifestos: Visions from the Information Revolutionaries*. New York, NY: TEXERE, 2002.
Brenner, Susan. *Cyberthreats: The Emerging Fault Lines of the Nation* State. New York, NY: Oxford University Press, 2009.
Clausewitz, Carl Von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.
Fadok, David. "John Boyd and John Warden: Airpower's Quest for Strategic Paralysis," in *The Paths of Heaven: The Evolution of Airpower Theory*. Edited by Colonel Phillip Melinger. Maxwell AFB, AL: Air University Press, 1997.
Fuller, Col J. F. C. *The Foundations of the Science of War*. London: Hutchinson & Co Publishers, Ltd: 1926; Reprint with permission of Harold Ober Associates.
Gilpin, Robert. *Global Political Economy: Understanding the Global Political* Order. Princeton, NJ: Princeton University Press, 2001.
Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz, eds. *Cyberpower and National Security*. Dulles, VA: National Defense University and Potomac Books, 2009.
Liang, Qiao and Xiansui Wang. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999. http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf (accessed 15 December 2009).
Libicki, Martin C. *Conquest in Cyberspace: National Security and Information Warfare*. New York, NY: Cambridge University Press, 2007.
Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. London: Frank Cass, 2004.
Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, DC: The National Academies Press, 2009.
Raymond, Eric S. *The Cathedral and the Bazaar*. O'Reilly Media, published under Open Publication License, ver 2.0, 2000. http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ (accessed 30 Nov 2009).

Schelling, Thomas. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.
Schelling, Thomas. *The Strategy of* Conflict. Cambridge, MA: Harvard University Press, 1980.
Shapiro, Carl and Hal R. Varian. *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press, 1999.
Sun Tzu. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York, NY: Oxford University Press, 2005.
Tapscott, Don and Anthony D. Williams. *Wikinomics: How Mass Collaboration is Changing Everything*. New York, NY: Penguin Group, 2006.
Toffler, Alvin. *The Third Wave*. New York, NY: Bantom Books, 1980.
Waltz. Kenneth. *Theory of International Politics*. Boston, MA: McGraw Hill, 1979.
White, Lynn. *Medieval Technology and Social Change*. New York, NY: Oxford University Press, 1966.

Briefings/Point Papers/Memos/Messages

Adaptive Cyber Security Instruments, Inc. "Stopping the Unstoppable – Your Best Line of Defense." Product overview. http://www.acsi-cybersa.com/Products.html (accessed 29 March 2010).
Alberts, David. "NEC2 Short Course – Module 2 Network-Enabled Capability." Course materials, 24 Jan 2010. http://www.dodccrp.org/files/nec2_short_course/NEC2%20Short%20Course%20Module%202%20-%20NEC2%20-%20%20Alberts%201-%2024%20-2010.pdf (accessed 8 Mar 2010).
Li, Jason and Peng Liu. "Bayesian Security Analysis: Opportunities and Challenges." Presentation to the ARO workshop, 14 Nov 2007. http://ist.psu.edu/s2/ARO-SA/ (accessed 29 March 2010).
Lookingglass Inc. "Scoutvision: The Industry's Most Reliable and Intuitive Cyber Intelligence Platform." Product overview. http://www.lgscout.com/products/scoutvision (accessed 29 March 2010).
Saydjari, O. Sami, et al. "Letter to President Bush." 27 Feb 2002. http://www.uspcd.org/letter.html (accessed 8 Mar 2010).
Symantec Inc. "Symantec Utilizes Security Intelligence and Experts to Deliver Cyber Threat Analysis Program." Product announcement, 28 Jul 2009. http://www.symantec.com/about/news/release/article.jsp?prid=20090728_01 (accessed 29 March 2010).

Government Documents

Department of Defense. "Capstone Concepts for Joint Operations," v3.0, 15 Jan 2009. http://www.dtic.mil/futurejointwarfare/concepts/approved_ccjov3.pdf (accessed 8 Mar 2010).

Department of Defense. "Dictionary of Military and Associated Terms." http://www.dtic.mil/doctrine/dod_dictionary/ (accessed 6 Mar 2010).

Department of Justice, Computer Crime and Intellectual Property Section. "Prosecuting Intellectual Property Crimes." 3rd edition, 2006. http://www.justice.gov/criminal/cybercrime/ipmanual/01ipma.html (accessed 7 May 2010).

Director, Force Transformation, Office of the Secretary of Defense. "The Implementation of Network-Centric Warfare." Washington, DC: 2005.

Garstka, John. "Network Centric Operations Conceptual Framework." Version 1.0, Nov 2003. http://www.iwar.org.uk/rma/resources/ncw/ncw-conceptual-framework.pdf (accessed 15 Dec 2009).

Garstka, John. "Network Centric Operations Conceptual Framework." Version 2.0 (draft), Jun 2004. Obtained from Margita Rushing at Evidence Based Research.

Joint Chiefs of Staff, Joint Publication 3-13. "Information Operations." 13 Feb 2006. http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 29 Mar 2010).

Joint Chiefs of Staff, Joint Publication 6-0. "Joint Communications Systems." 20 Mar 2006. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf (accessed 6 Apr 2010).

National Security Council. "The Comprehensive National Cybersecurity Initiative." http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 29 May 2010).

National Institute of Standards and Technology, "The Security Content Automation Protocol," scap.nist.gov (accessed 29 May 2010).

Rumsfeld, Donald. "Military Strategy for Cyberspace Operations." 11 Dec 2005. http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf (accessed 6 April 2010).

Personal Communications – Interviews/E-Mails

Garstka, John. Interviews with the author 30 Dec 2009, 14 Jan 2010, 8 Feb 2010, and 18 Feb 2010 and e-mails to the author 14 Jan 2010 and 5 Feb 2010.

Guevin, Lt Col Paul R (Air Force Space Command/A3I). Interview with the author 19 Feb 2010.

Myers, Maj Robert (Joint Task Force-Global Network Operations). E-mail to the author, 5 Mar 2010.

Wile, Danette (Joint Task Force-Global Network Operations liaison to 24th Air Force). Interview with the Author, 19 Feb 2010.

Reports

Department of Defense. "Network Centric Warfare Report to Congress." Jul 2001. http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf (accessed 8 Mar 10).

Gonzales, Daniel, et al. "Network Centric Operations Case Study: Air-to-Air Combat With and Without Link 16." Santa Monica, CA: RAND, 2005.

Gonzales, Daniel, et al. "Network Centric Operations Case Study: The Stryker Brigade Combat Team." Santa Monica, CA: RAND, 2005.

"NATO Code of Best Practice for C2 Assessment." Washington, DC: Command and Control Research Program, Oct 2002. http://www.dodccrp.org/files/NATO_COBP.pdf (accessed 24 Mar 2010).

"NATO Code of Best Practice for C2 Assessment: Analyst's Summary Guide" Washington, DC: Command and Control Research Program, 2002. http://www.dodccrp.org/events/12th_ICCRTS/CD/library/html/pdf/NATO_Analyst.PDF (accessed 24 Mar 2010).

National Institute of Standards and Technology, Special Publication 800-30. "Risk Management Guide for Information Technology Systems." Gaithersburg, MD: National Institute of Standards and Technology, Jul 2002. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (accessed 24 March 2010).

National Institute of Standards and Technology, Special Publication 800-94. "Guide to Intrusion Detection and Protection Systems." Gaithersburg, MD: National Institute of Standards and Technology, Feb 2007. http://csrc.ncsl.nist.gov/publications/nistpubs/800-94/SP800-94.pdf (accessed 24 March 2010).

Speeches

Chilton, General Kevin, USAF. Speech to the United States Air War College, 10 March 2010.

Mattis, General James, USMC. Statement before the House Armed Services Committee, 18 Mar 2009. http://smallwarsjournal.com/blog/2009/03/general-james-mattis-before-th/ (accessed 8 March 2010).

Saydjari, O. Sami. "Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action." Testimony before the House Committee on Homeland Security, subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, 25 April 2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf (accessed on 9 Mar 2010).